Cyber Range: Preparing for Crisis or Something Just for Technical People?

Jani Päijänen[1], Karo Saharinen[1], Jarno Salonen[2], Tuomo Sipola[1], Jan Vykopal[3] and Tero Kokkonen[1]
[1]JAMK University of Applied Sciences, Jyväskylä, Finland
[2]VTT Technical Research Centre of Finland, Tampere, Finland
[3]Masaryk University, Brno, Czech Republic
jani.paijanen@jamk.fi
karo.saharinen@jamk.fi
jarno.salonen@vtt.fi
tuomo.sipola@jamk.fi
vykopal@ics.muni.cz
tero.kokkonen@jamk.fi
DOI: 10.34190/EWS.21.012

Abstract: Digitalization has increased the significance of cybersecurity within the current highly interconnected society. The number and complexity of different cyber-attacks as well as other malicious activities has increased during the last decade and affected the efforts needed to maintain a sufficient level of cyber resilience in organisations. Due to Industry 4.0 and the advanced use of IT and OT technologies and the adaptation of IoT devices, sensors, AI technology, etc., cybersecurity can no longer considered to be taken lightly when trying to gain a competitive advantage in business. When transferring from traditional reactive cybersecurity measures to proactive cyber resilience, cyber ranges are considered a particularly useful tool for keeping the organisation in the game. With their background in defence research (e.g., DARPA NCP in 2008), cyber ranges are defined as interactive simulated platforms representing networks, systems, tools, and/or applications in a safe, legal environment that can be used for developing cyber skills or testing products and services. Cyber ranges can be considered vital in facilitating and fostering cybersecurity training, certification, and general education. Despite the definition, cyber ranges seem to be only used by military or so-called "technical people" when quite a few more organisations could benefit from them. This article attempts to reveal the secrets behind cyber ranges and their use focusing on suitable target environments, common functions, and use cases. Our main objective is to identify a classification of cyber ranges and skills related to these diverse types of ranges. We emphasise the cyber resilience of any type of organisation that demands the use of cyber range type of training. Different training scenarios improve different sets of organisational skills. The article is based on an extensive survey on cyber ranges, their use, and technical capabilities that was conducted in CyberSec4Europe project.

Keywords: cyber range, cyber resilience, cyber training, organisational skills, cybersecurity

1. Introduction

Given the concept of a cyber crisis (or even cyber war), one has to imagine a cyber weapon being used in a cyber-attack, for example of a malware program or a denial-of-service attack. This attack is usually directed towards a victim (organization or person) that is facing a crisis situation. Different countries have different laws protecting the victim against this kind of aggression. Outside the realm of cyber security, there are usually various kinds of laws prohibiting and restricting the usage of physical weapons, even to the point of having specialized physical shooting ranges abiding the law (Ministry of Interior, Finland, 1998/2003) for the practice of regular weaponry. In the cyber context, these kinds of cyber weapon shooting ranges are being formed as cyber arenas or cyber ranges; however, the development of regulations on how these platforms should be used is currently lacking.

Cyber ranges (or cyber arenas) are technical platforms that facilitate education, training, and exercise of cyber security (Karjalainen and Kokkonen, 2020a). According to Russo, Costa and Armado (2020), these ranges are complex infrastructures that simulate real-world cybersecurity scenarios. These technical platforms have developed in different organizations simultaneously from smaller technical laboratory environments to cloud-based solutions. They might have originally been platforms used to demonstrate products and technology, or even mirroring a technical production network to act as an introductory platform for new employees. Ukwandu et al (2020) have identified current trends, types, target domains and technologies used in cyber ranges and testbeds. On the other hand, the definition of cyber ranges does not limit or restrict use cases, target groups, or participant roles utilizing a cyber range (ECSO, 2020).

2. At whom cyber ranges are targeted?

Cyber ranges can be used for training or educating individuals or groups of people such as employees of companies or organisations. They can be used for cyber security research and development, hosting various kinds of events, certifying products or services, performing competence assessment, or recruiting people (ECSO, 2020; Yamin, Katt, and Gkioulos, 2020). Some cyber ranges can be used to train cyber defence (NATO CCDCOE, 2020; Vykopal at al, 2017). Events in a cyber range can be cyber security exercises or competitions targeted at a company (FINGRID, 2017), an organisation (Valtori, 2020; MITRE, 2014), international (NATO CCDCOE, 2020), or national cyber security exercises (Secretariat of the Security Committee, 2019). An exercise can target a specific audience without any shared training or background (CyberSec4Europe, 2021). Also, various cyber security related competitions such as Capture the Flag (CTF) competitions targeted at individuals or teams can be organised as a cyber range event. Firstly, the following sections introduce target groups benefiting from cyber ranges and secondly, use cases that the cyber ranges have supported.

2.1 Target groups

Individuals, Personal Knowledge, Skills and Abilities (KSA)

Cyber ranges offer a technical environment where citizens can train their understanding of the cybersecurity phenomena. The European Union has produced the European Qualifications Framework (EQF), which helps to improve transparency, comparability, and portability of people's qualifications between the nations in the EU. These qualifications are listed as learning outcomes Knowledge, Skills and Abilities (KSAs). Cyber ranges could be used in a Cyber Security Massive Open Online Course (MOOC) implementation (Fischer-Hübner et al., 2020), where the MOOCs offer a platform for everyone to improve their KSAs.

Curriculum students

These KSAs are developed through degree programmes following a curriculum suited for the respected EQF level. Curriculum students of higher education (Karjalainen, Kokkonen and Puuska 2019; Saharinen et al, 2019; Karjalainen and Kokkonen, 2020b) are sometimes required to pass courses that utilize these cyber ranges. Regardless these courses being either a mandatory or elective part of their studies, many education and research organizations are developing the capability (Frank et al, 2017) to host courses through these environments as the demand for capable workforce increases constantly in the field of Cyber Security.

Companies

Companies invest in protecting their environments, as digitalization is forcing them to be increasingly available online both in the private and public sectors. To uphold these availability requirements, companies need to employ a capable workforce provided by the education sector (Bell and Oudshoorn, 2018). Students with practical knowledge of handling a live cyber crisis are often valued, and the capability of upholding the cyber presence of a company simultaneously with a cyber crisis can be seen as a part of the cyber resilience of a nation.

Law enforcement

Additionally, individuals face the problem of a cyber crisis when e.g., their digital identity is stolen, or payment frauds are committed in the e-banking realm (Singh and Rastogi, 2018). In both companies and individual cases, these cyber crises end up in police cybercrime statistics. Cybercrimes are investigated by specialized police units that survey and handle cybercrimes for prosecution. Exact methods of cybercrime investigation are still a developing field, which also means the police forces need an educational environment for investigating cybercrimes.

Government

If the cyber crisis that either faces companies or individuals exceeds a certain threshold, a nation has to implement its laws and regulations to enter a state of war (Sevis and Seker, 2016). This means, depending on the country in question, that the military can start protecting its civilians and assets, be they physical or cyber.

After these laws or regulations are invoked, the protection of assets is commonly left to the nation's military forces.

Military cyber defence capabilities

The Defence Forces of different countries have been mentioned to use National Cyber Ranges: Norway (NTNU, 2018), Estonia (Republic of Estonia Centre of Defence Investment, 2020) and Finland (JYVSECTEC, 2017; EU2019.fi, 2019) to name a few. Additionally, multinational coalitions have practiced in self-contained cyber ranges brought about for the need, for example, Locked Shields (NATO CCDCOE, 2020). Different military forces have stated that cyber is the fifth domain of warfare after land, sea, air, and space (NATO, 2016).

Researchers

All the aforementioned entities have Cyber Security researchers (ENISA, 2020a; 2020b; 2020c) working separately and in coalition on different research projects. The development of cyber ranges as such is a less researched area, as the phenomena and results after working in the cyber range are typically more sought after.

2.2 Use cases for cyber ranges

Security research, testing, development, and certification: Development testbeds, research environments, and certification tracks have been used in the industry for longer than the term Cyber Range has existed. Development testbeds are usually set up by development teams to see how their updates work in an environment mimicking the production environment. Research environments aim at closeness to the real thing, or a phenomenon is researched by scientists, often relying on ICT environments separated from the Internet. Certification bodies require that the test samples pass through a set of phases on a track in order to gain a label of quality provided by the entity awarding the certificates.

Security Education through Competence Building and Assessment: Competence building follows the said certification bodies to offer practicing environments, i.e. cyber ranges, for students trying to reach validation for their skills. This thought has brought up the environment itself to be an active area for student assessment how their competence has developed while working within the environment.

Development of Cyber Capabilities and Resilience: The earlier mentioned competence building is a part of an individual's growth as an expert. The development of cyber capabilities and resilience looks at the phenomenon, outcomes using a cyber range, from the organisation´s viewpoint, e.g. Fingrid, 2017. One part of it is recruitment, where organizations look for competent workforce, and the interview process might have recruitment sections handled in a technical cyber environment. Additionally, ongoing personnel might be trained using organizational exercises.

Cross-domain development environment (Digital Dexterity): The digital dexterity of the whole domain is developed when multiple organisations from multiple industries participate in a cyber range dedicated to the particular industries. These exercises usually show the weak points of processes in multiple organizations, e.g., supply chain processes.

National and International Cybersecurity Competitions or Exercises: National or international cybersecurity competitions, in which individuals, organizations or nations compete against one another as well as national and international cyber security exercises, may both advance all the aforementioned use cases.

3. Cyber range usage based on a survey

In this section, we analyse the data from a conducted cyber range survey. The survey was conducted in the CyberSec4Europe project, and it was open from 23 April 2020 to 27 May 2020. A total of 44 responses were received, of which 39 responses were considered valid. The number of survey responses, 39, is considered valid based on the survey authors' experience in the subject. In the survey terms, we decided not to publish any cyber range specific features and capabilities. The survey consisted of single-choice, multiple-choice and open questions, and it did not contain any mandatory fields. (CyberSec4Europe, 2020)

3.1 Cyber range target groups

The survey data had a total of seven target groups (TGs) listed, and respondents provided three additional target groups. Hence, the data comprised a total of ten target groups: General public, Secondary level students, Degree program students (Bachelor's or Master's degree students), Government organizations, Companies and Enterprises, Non-profit associations or similar, Other, and respondent reported Training Service Providers, Systems Integrators, and Cyber Professionals. The respondents belonged to the following target groups: Training Service Providers, Systems Integrators and Cyber Professionals. They are presented in the columns of Figure 1. The most represented target groups were Companies and Enterprises 77% (30), Degree program students (Bachelor or Master's degree students) 59% (23), Government organizations 59% (23), Non-profit associations or similar 23% (9), General Public 18% (7) and Secondary level students 18% (7). The following groups were represented in the data by just one respondent: Training Service Providers, Systems Integrators, Cyber Professionals and Other. The top 20% of the cyber ranges supported four or more target groups.

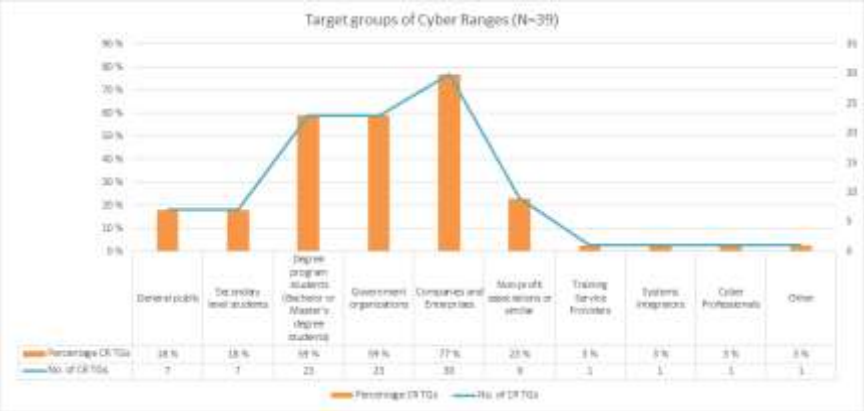

Figure 1: Distribution of target groups (N=39)

The number of target groups supported by cyber ranges is shown in Figure 2. Single Target Group was reported by 23% (9), two target groups by 28% (11), three target groups by 26% (10), four target groups by 13% (5), five target groups by 5% (2), and six target groups by 5% (2). Based on the survey data, a cyber range supports two (2.6) target groups on average.

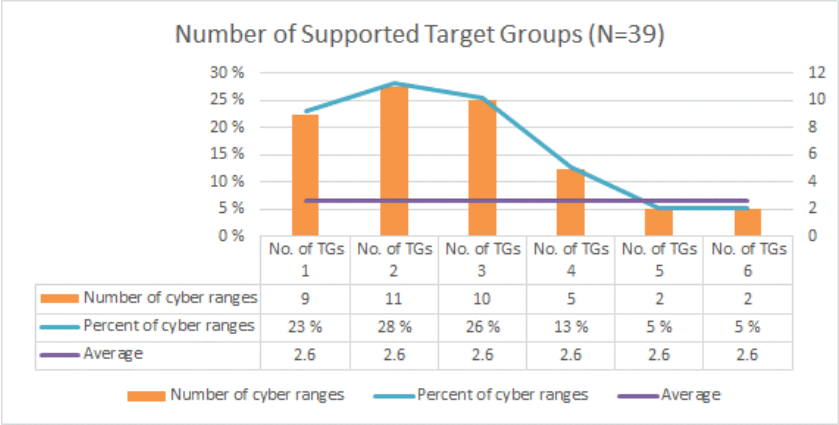

Figure 2: Number of supported target groups (N=39)

3.2 Cyber range use cases

A cyber range may be dedicated to a single use case, or it may support multiple use cases. The survey data contained 11 use cases, namely Security testing and certification, Security research & development, Competence Building, Security Education, Development of Cyber Capabilities, Development of Cyber Resilience, Competence Assessment, Recruitment, Cross-domain development environment (Digital dexterity), National and International Cybersecurity Competitions, and National and International Cybersecurity Exercises. The reported use cases were distributed (Figure 3) as Security testing and certification 44% (17), Security research & development 72% (28), Competence Building 62% (24), Security Education 82% (32), Development of Cyber Capabilities 51% (20), Development of Cyber Resilience 38% (15), Competence Assessment 36% (14),

Recruitment 13% (5), Cross-domain development environment (Digital dexterity) 13% (5), National and International Cybersecurity Competitions 26% (10), National and International Cybersecurity Exercises 44% (17).

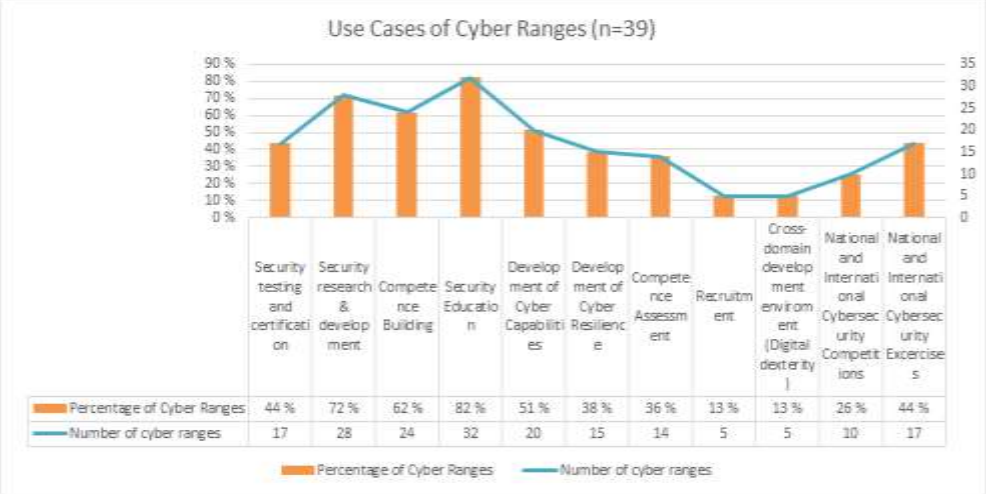

Figure 3: Distribution of use cases (N=39)

Figure 4 displays the number of the use cases (No. of UCs) supported by the cyber ranges. All eleven use cases were supported by 5% (2), ten use cases by 5% (2), nine use cases by 5% (2), eight use cases by 3% (1), seven use cases by 10% (4), six uses cases by 10% (4), five use cases by 10% (4), four use cases by 10% (4), three use cases by 13% (5), two use cases by 13% (5), one use case by 15% (6) cyber ranges as reported by the respondents. On average, a cyber range supports four (4.79) use cases. The top 20% of cyber ranges supported eight or more use cases.

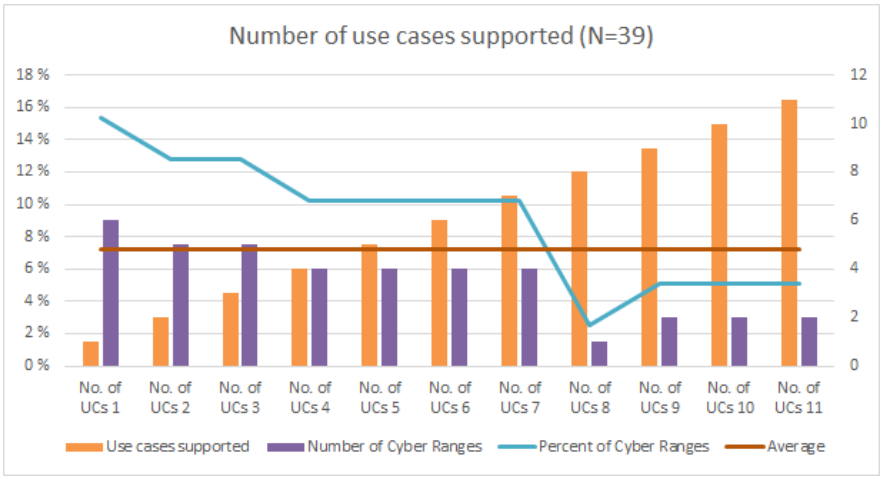

Figure 4: Number of use cases supported by cyber ranges (N=39)

3.3 Cyber range participant roles

Six user roles were listed: Director (Business, Director, Communication, etc.), Developer, Researcher, Security professional, Educator, and Other. The survey respondents reported to option "Other" with the following: Sysadmin, Network admin, Student, Job Applicants, Employees, Domain specialist. Two respondents responded "Different roles from organisations which are responsible for some parts of cyber incident response & handling (e.g. Public relations, Process owners, System owners, Technical specialists)" and "CISO, Incident managers, depending on the roles in organisations (e.g. IT admins)."

The number of participant roles is shown in Figure 6: one role 21% (8), two roles 23% (9), three roles 28% (11), four roles 13% (5), and five roles 13% (5). One respondent (3%) did not report the number of participant roles. On average, a cyber range supports two participant roles (2.66%). No cyber ranges were reported to support all roles, including the "Other" role.

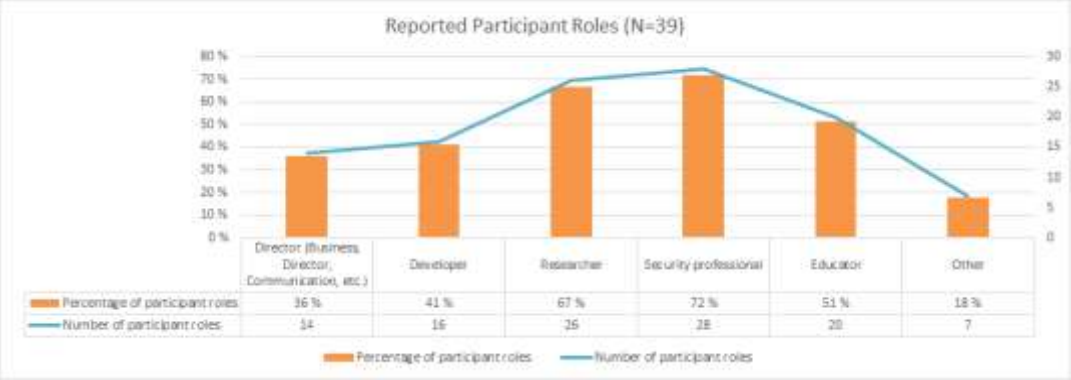

Figure 5: Distribution of participant roles

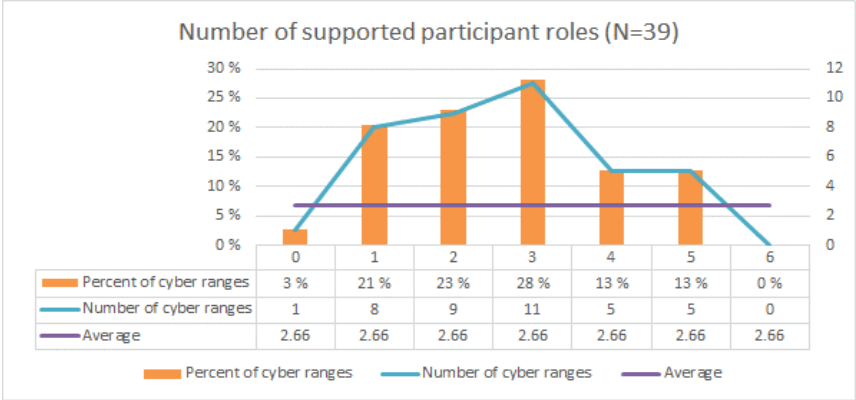

Figure 6: Number of participant roles supported (N=39)

3.4 Cross-tabulation of cyber range use cases and participant roles

Table 1 shows the cross-tabulation of filtered data, where target groups were Government organizations, Companies and Enterprises, or Non-profit associations or similar. It shows which use cases a cyber range supports, and the user roles supported. The table rows represent use cases and the columns the user roles. The number following a use case reports the total number of times the use case was reported: Security testing and certification (57), Security research & development (90), Competence Building (75), Security Education (85), Development of Cyber Capabilities (62), Development of Cyber Resilience (50), Competence Assessment (47), Recruitment (20), Cross-domain development environment (Digital dexterity) (21), National and International Cybersecurity Competitions (35), National and International Cybersecurity Exercises (54). In total, the user roles shown in the table were reported as follows: Director (Business, Director, Communication, etc.) 83 times, Developer 94 times, Researcher 145 times, Security professional 161 times, Educator 106 times, and Other User Roles seven times. In each use case the reported cyber ranges supported all the roles, except Other User Roles.

Table 1: Cross-tabulation of use cases with participant roles, filtered.

Use case	Director	Developer	Researcher	Security professional	Educator	Other User Roles	Total
Security testing and certification	8	10	14	14	11	0	57
Security research & development	11	15	22	20	15	7	90
Competence Building	9	12	18	22	14	0	75
Security Education	11	12	21	24	17	0	85
Development of Cyber Capabilities	10	10	15	17	10	0	62
Development of Cyber Resilience	8	8	11	14	9	0	50
Competence Assessment	6	7	11	14	9	0	47
Recruitment	3	3	5	5	4	0	20
Cross-domain development enviroment (Digital dexterity)	4	4	5	5	3	0	21
National and International Cybersecurity Competitions	4	5	10	10	6	0	35
National and International Cybersecurity Excercises	9	8	13	16	8	0	54
Total	83	94	145	161	106	7	596

4. Discussion

According to the research data, cyber ranges had various target groups (Figure 1), and the supported participant roles of cyber ranges were not limited to technically oriented user roles, but there were roles for e.g., directors (Figure 5). The cyber ranges supporting directors as a potential participant role, support a broader spectrum of use cases (Table 1). The data indicates that cyber ranges were used by both technical and non-technical user roles.

When an entity, e.g., an organisation, a company or an individual faces a cyber incident, it does not require only technical skills to understand, resolve and respond to the incident but also non-technical skills are required (Fingrid, 2017). An organisation may establish a Cyber Security Incident Response Team (CSIRT) that tries to respond to and resolve the attack. According to Onwubiko and Ouazzane (2020), CSIRTs should have the necessary expertise and support from the infrastructure and networking teams, systems administration and management teams, business continuity and disaster recovery teams, communications and press office, and designated senior management teams. In case of severe enough incident, senior management could provide decision-making and funding support; a cyber incident may require a dedicated cost-budget that only the senior management can allocate. The CSIRT example and exercising or training for incidents can be seen as preparing for a local and limited duration crisis. The work to recover from a cyber incident may last long, even several months, depending on the size of the organisation. In larger organisations, the CSIRT team contains these dedicated roles.

In conclusion, the key question of this article “Are cyber ranges just for technical people or do they actually provide vital tools for the organisation to prepare against a crisis?”, we might say that based on our research results, cyber ranges enable the organisations to carry out more than just technical mitigation measures. However, this highly depends on the decisions made by the organisation itself on how well they take the different functionalities into use and make full use of the platform. Simply said, a cyber range acquired only for a specific technical purpose might be somewhat limited in terms of functionality. Since there are quite a few cyber range platforms available on the market with various features ranging from single technical point solutions to comprehensive cyber arenas including realistic simulation of business processes and technical systems, selecting the right tool for a specific organisation might require thorough examination of available options and possibly even external consultation.

The research results show that some cyber ranges support or have participated in national or international cybersecurity exercises. Such exercises, when exercising joint operations of civil government and authorities, or security authorities, require there to be non-technical participants, so that the areas of responsibilities as stated by national or international laws are followed.

Individuals, cyber professionals, government organisations, companies and enterprises, and degree program students use cyber ranges for competence building and development. The business features and domains as well as the technical features and functionalities they provide for users should be researched further. As the original survey was not specifically designed for the purpose of analysing the scope of educational cyber range use, there is a definite need for a new survey. The questions should be adjusted so that their scope focuses more on the previously studied subject and perhaps includes multiple different subjects. Future research might focus on the features, functionalities and properties of cyber ranges which have been reported to support non-technical roles for a better understanding of the potential use cases that they could participate for.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgments

This research was supported by the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project of the Horizon 2020 SU-ICT-03-2018 program, and by the ERDF project “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

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

References

Bell S. and Oudshoorn M. (2018) "Meeting the Demand: Building a Cybersecurity Degree Program with Limited Resources," *2018 IEEE Frontiers in Education Conference (FIE)*, San Jose, CA, USA, 2018, pp. 1-7, DOI: 10.1109/FIE.2018.8659341.

CyberSec4Europe. (2020) "D7.1 Report on existing cyber ranges, requirements", [online], Cyber Security for Europe (CyberSec4Europe), 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

CyberSec4Europe. (2021) "CyberSec4Europe Hosting Flagship 1: An Online Cybersecurity Exercise", [online], Cyber Security for Europe (CyberSec4Europe), https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/

ECSO. (2020) Understanding Cyber Ranges: From Hype to Reality. [Online]. Available at: https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf, European Cyber Security Organisation (ECSO), Brussels, Belgium.

ENISA. (2020a) "ENISA Threat Landscape 2020 - Insider Threat". ISBN:978-92-9204-354-4. DOI:10.2824/552242

ENISA. (2020b) "ENISA Threat Landscape 2020 - Main incidents", [online], European Union Agency for Network and Information Security (ENISA), Science and Technology Park of Crete (ITE), Heraklion, Greece, Heraklion, Greece, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2020c) "ENISA Threat Landscape 2020 - The year in review", [online], European Union Agency for Network and Information Security (ENISA), Science and Technology Park of Crete (ITE), Heraklion, Greece, Heraklion, Greece, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

FINGRID magazine. (2017) "Cyber security is ensured with genuine exercises, [online], Fingrid Oyj, https://www.fingridlehti.fi/en/cyber-security-ensured-genuine-exercises/

Finnish Ministry of Interior. (2015). "Firearms Act", [Online], https://www.finlex.fi/fi/laki/kaannokset/1998/en19980001.pdf.

EU2019.fi (2019) "Cyber Ranges Federation – Towards Better Cyber Capabilities Through Cooperation" [online], Finnish Presidency of the Council of the European Union (EU2019.fi), https://eu2019.fi/en/-/cyber-ranges-federation-yhteistyolla-kohti-parempaa-kyberkyvykkyytta

Fischer-Hübner S. et al. (2020) Quality Criteria for Cyber Security MOOCs. In: Drevin L., Von Solms S., Theocharidou M. (eds) Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology, vol 579. Springer, Cham. https://doi.org/10.1007/978-3-030-59291-2_4

Frank, M., Leitner, M. and Pahi, T. (2017) "Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 38-46, DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23.

JYVSECTEC (2017) "JYVSECTEC success story", [online], Jyväskylä Security Technology (JYVSECTEC), https://jyvsectec.fi/2017/02/jyvsectec-success-story/

K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), London, 2016, pp. 1-9, DOI: 10.1109/CyberSecPODS.2016.7502348.

Karjalainen, M., Kokkonen T. and Puuska, S. (2019) "Pedagogical Aspects of Cyber Security Exercises", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, pp 103–108. DOI: 10.1109/EuroSPW.2019.00018

Karjalainen, M. and Kokkonen, T. (2020a) "Comprehensive Cyber Arena; The Next Generation Cyber Range", 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 11–16. DOI: 10.1109/EuroSPW51379.2020.00011.

Karjalainen, M. and Kokkonen, T. (2020b) "Review of Pedagogical Principles of Cyber Security Exercises", Advances in Science, Technology and Engineering Systems Journal, Vol 5, No 5, pp 592–600. DOI: 10.25046/aj050572.

NATO. (2016) "NATO Cyber Defence" [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

NATO CCDCOE. (2020) "Exercises", [Online]. Available at: https://ccdcoe.org/exercises/.

NTNU. 2018. Norwegian University of Science and Technology. "Norwegian Cyber Range". https://www.ntnu.no/ncr

Onwubiko C., Ouazzane, K. (2020) "SOTER: A Playbook for Cybersecurity Incident Management", IEEE Transactions on Engineering Management, DOI: 10.1109/TEM.2020.2979832.

Republic of Estonia Centre of Defence Investment. 2020. "Estonia Signs Contract to Develop Command Platform for NATO Cyber Range". [Online]. Available at: https://www.kaitseinvesteeringud.ee/en/estonia-signed-a-contract-for-the-development-of-a-command-platform-for-the-nato-cyber-range/

Russo, E., Costa, G, Armado, A. (2020) "Building next generation Cyber Ranges with CRACK", Computers & Security, Vol 95, pp. 101837. DOI: 10.1016/j.cose.2020.101837.

Singh S. K. and Rastogi N. (2018). "Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018, pp. 1-6, DOI: 10.1109/IoT-SIU.2018.8519884.

Saharinen K., Karjalainen M., and Kokkonen T. (2019) “A Design Model for a Degree Programme in Cyber Security”. In Proceedings of the 2019 11th International Conference on Education Technology and Computers (ICETC 2019). Association for Computing Machinery, New York, NY, USA, 3–7. DOI: 10.1145/3369255.3369266

Secretariat of the Security Committee. (2019) “Turvallisuusviranomaiset kehittävät osaamistaan kansallisessa kyberturvallisuusharjoituksessa”, [Online]. Available at: https://turvallisuuskomitea.fi/tiedote-turvallisuusviranomaiset-kehittavat-osaamistaan-kansallisessa-kyberturvallisuusharjoituksessa-kyha19-jamkissa-jatkossa-myos-terveydenhuollon-toimijat-mukaan-harjoituksiin/

Ukwandu, E., Ben Farah, M.E., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis C., Bures M., Andonovic, I., Bellekens, X. (2020) “A Review of Cyber-Ranges and Test-Beds: Current and Future Trends”, arXiv preprint arXiv:2010.06850.

Valtori. (2020) “Valtori’s 2019 financial statements published”, [Online]. Available at: https://valtori.fi/en/-/valtorin-tilinpaatos-2019-julkaistu?languageId=en_US

Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M., Tovarňák, D. (2017) “KYPO Cyber Range: Design and Use Cases”, Proceedings of the 12th International Conference on Software Technologies - Volume 1: ICSOFT, SciTePress, Madrid, Spain, pp. 310-321. DOI: 10.5220/0006428203100321.

Yamin, M.M., Katt, B. and Gkioulos, V. (2020) “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture”, Computers & Security, Vol 88, pp. 101636. DOI: 10.1016/j.cose.2019.101636.