Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D7.1

Report on existing cyber ranges, requirements

Document Identification	
Due date	31.08.2020
Submission date	31.08.2020
Revision	1.0

Related WP	WP7	Dissemination Level	Public
Lead Participant	JAMK	Lead Authors	Elina Suni (JAMK) Juha Piispanen (JAMK) Jarmo Nevala (JAMK) Jani Päijänen (JAMK) Karo Saharinen (JAMK)
Contributing Beneficiaries	BRNO, VTT, UMU	Related Deliverables	

Abstract:
PART A of this deliverable provides a report on existing cyber ranges, requirements from industry and vertical sectors. The report is based on our research survey and interviews of respondents, which indicated what they have done with cyber ranges and possibly their federation. Respondents to the survey were mainly from Europe, but also valid responses were received also from Australia, Canada, Israel and United States.

PART B of this report contains requirements of connections and services including specification for implementation. Targeted technology was open-source SD-WAN technology. The demonstration of the specification will be delivered at later project phase. Target audience for requirement specification are cyber range specialists and network specialists.

In this document, we also propose more fine-grained definitions for cyber range federation: Operational Federation and Technical Federation. This distinction showed critical during the course of work on the deliverable, namely in the discussions with experts working with cyber ranges on daily basis.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This deliverable analyses results from a conducted online survey and follow-up interviews of users, operators, and developers of cyber ranges. The goal of the survey was to gain understanding on existing cyber ranges and those under development, their use cases, capabilities and capacity. Based on the survey results, we identified use cases for cyber range technical federation and based on them we propose a set of requirements, which will enable the implementation of the use cases.

European Cyber Security Organisation (ECSO) defines cyber range as follows:

> *A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. 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.* (ECSO, 2020)

Interestingly, the survey's results show that only rare cyber range vendors, operators or consultants utilize cyber ranges themselves. The survey and interview results show that cyber ranges are not only used for developing individuals' skills and knowledge but also to train and exercise organisations or companies and their service providers to develop their cyber resilience. In addition, cyber ranges were used for cyber security research and development, testing and certification. Therefore, an interesting question for future research is to study if cyber range suppliers, operators and consultants have developed their own cyber resilience.

The results of the survey show there are no universal certification requirements for cyber ranges, the facilities or the networks on which they run, nor for the staff developing, operating, and maintaining them. For the customers it is hard to compare cyber ranges features and functionalities, capabilities and capacity due to the shortcoming of current cyber range taxonomies and classification. Therefore, a customer should consider if a cyber range is able to simulate the target scenario in a way that is sufficiently realistic to implement the planned cyber exercise and to achieve the wished training goals.

During the work of this deliverable and in the related discussions, considering also, the ECSO report "Understanding cyber ranges: From hype to reality" (ECSO, 2020); it was clear that the term Cyber Range Federation does not have a universally accepted meaning. The ECSO report clearly defines cyber ranges, and has other advantages as well, but in our opinion, it has a mixed definition for cyber range federation. During our work, we noticed that sometimes the meaning was even in conflict with the established definition widely used in the IT domain. Therefore, we propose more fine-grained terms to be used discussing cyber range federation: Operational Federation and Technical Federation. Operational Federation refers to the sharing of operative cyber exercise or scenario data, or cyber range configuration data in machine-readable format, between cyber range operators or parties using them. 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. Once the technical federation is established, the usage of the resources or services may happen seamlessly, i.e. transparently from end user perspective. It may require contracts or other kinds of a trust relationship where the parties agree e.g. acceptable usage of provided functionalities or services. It does not mean that two or more federated data center services are connected together, i.e. they are not integrated. Using either the operational or the technical federation does not imply that the other one should be used.

Part A of this document contains a report on existing cyber ranges, and interviews of selected respondents, and states requirements from industry and vertical sectors from within the CyberSec4Europe project. The beginning of the Part A is intended for audience with little previous knowledge or experience in cyber ranges. The survey results part covers the generic cyber range related analysis.

Part B of this document contains the requirements specification for the cyber range *technical* federation. The intended audience for the requirement specification part includes cyber range technical specialists and network specialists. The conclusions of the whole document are included at the end of Part B.

Document information

Contributors

Name	Partner
Jarno Salonen	VTT
Jan Vykopal	BRNO
Antonio Skarmeta	UMU
Marko Vatanen	JAMK

Reviewers

Name	Partner
Jozef Vyskoc	VAF
Christos Douligeris	UPRC
Bruno Crispo	UNITN
Vashek Matyas	BRNO

History

Version	Date	Authors	Comment
0.1	2020-06-16	Jani Päijänen	Added reference to the ECSO document, made minor modifications to the document metadata.
0.2	2020-06-18	Elina Suni Jani Päijänen	Updated text, made modifications to text, added proposal of TF and OF.
0.4	2020-06-26	Elina Suni Jani Päijänen	Merged document parts into a single document.

0.5	2020-06-29	Jani Päijänen	Added the interview results Sent the document for task force internal review.
0.6	2020-06-29	Jani Päijänen	Modifies the layout of the glossary of terms. Added chapter 8.8: Requirements for technical federation of cyber ranges
0.7	2020-07-02	Elina Suni Jani Päijänen	Incorporated comments from BRNO, updated Conclusion, Performance reporting and Connectivity subchapters.
0.8	2020-07-02	Jani Päijänen Elina Suni	Added executive summary for PART B.
0.9	2020-07-07	Jani Päijänen	Incorporated comments from Jarno / VTT. Added two new combinational charts: Training duration combinations and Combination of selected integration and federation technologies. Incorporated comments from external reviewer. Added figures of existing cyber range or service providers for survey questions.
0.93	2020-07-24	Jani Päijänen	Updated document according to review comments.
0.94	2020-08-02	Jani Päijänen	Updated document according to review comments. Executive summary of deliverable updated. Added Executive summary for Part A. Updated list of acronyms and glossary. Updated syntax for figure texts in many parts of document. Updated Part B contents to distinguish cyber exercise scenarios from use scenarios and connectivity scenarios.
1.00	2020-08-28	Jani Päijänen	Updated document version number.
1.00	2020-08-31	Ahad Niknia	Final check and submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
	AR	Augmented Reality
B	**BGP**	Border Gateway Protocol
C	**CPE**	Customer premises equipment
	CR	Cyber Range
	CS4E	CyberSec4Europe project
D	**DNS**	Domain Name System
E	**ECSO**	European Cyber Security Organisation
F	**FW**	Firewall
I	**ICS**	Industrial Control Systems
	ICT	Information and Communication Technology
	IoT	Internet of Things
	IP	Internet Protocol
	IPSEC	Internet Protocol Security
	IPv4	Internet Protocol version 4
	IPv6	Internet Protocol version 6
	IT	Information Technologies
	ISP	Internet Service Provider
M	**MPLS-VPN**	Multiprotocol Label Switching based VPN
N	**NAT**	Network Address Translation
	NTP	Network Time Protocol
O	**ORG**	An organization
	OT	Operational Technology
P	**PKI**	Public Key Infrastructure
R	**RTT**	Round-Trip Time
S	**SDN**	Software-defined Network
	SSH	Secure Shell
	SSL	Secure Sockets Layer
V	**vCPE**	Virtual Customer Premises Equipment
	VPLS	Virtual Private Lan Service
	VPN	Virtual Private Network
	VR	Virtual Reality

Glossary of Terms

B

Blue team

The blue team is the training audience of a cyber exercise. An exercise can include multiple blue teams from one organization or from multiple organizations. A blue team can include personnel from multiple levels of an organization or organizations.

Connectivity Scenario

A Connectivity scenario describe how cyber ranges utilizes the overlay network implemented in the cyber range technical federation in order to offer services, functionalities, features, capabilities or capacity to federation party's environment. It assists to answer to the question, for example, how exactly could one interconnect a service from a small-scale cyber range with a full-scale cyber range.

C

Cyber exercise

A cyber exercise is a planned event during which an organisation simulates cyber-attacks or information security incidents or other types of disruptions in order to test the organisation's cyber capabilities, from being able to detect a security incident to the ability to respond appropriately and minimise any related impact. (European Cyber Security Organization (ECSO) 2020)

Cyber Exercise professional

A Cyber exercise professional is a person of capable of planning cyber exercises and scenarios, executing and conducting them.

Cyber range

A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend on. 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. (European Cyber Security Organization (ECSO) 2020)

Cyber range federation

Cyber range federation means inter-operation of two or more distinct and formally disconnected cyber ranges which may have different network topologies and use cases.

Cyber range integration

Cyber range integration refers to a group of two or more cyber ranges which can communicate with one another to deliver a simulation environment spread across these cyber ranges. The integration between cyber ranges is usually achieved through traditional integration methods, such as VPN tunnels. Using such technologies requires that the integrated IP address spaces from across the different cyber ranges are different, in order to enable cyber ranges to transfer data between each *other*. (ECSO, 2020)

Cyber range operator

A cyber range operator is an organisation or a group of people in an organisation, which operates a running cyber range, being responsible for the technical aspects of the range.

Cyber range professional

Cyber range professional is a person who develops, maintains and modify or customise cyber range platform or the instance of it. For example, the person may modify or upgrade the infrastructure, network topology, relocate service in the cyber range network, or deploy new services for the operating organisation or for customer organisation. In the context of small-scale cyber ranges, they may be referred as laboratory engineers or with similar title.

Cyber range vendor

A cyber range vendor is an organisation or a group of people in an organisation, which develops a technical solution and provides requirements for facilities and the use and operating environment, which can be used for cyber exercises and trainings. The vendor can be a commercial third-party or an in-house virtual organisation.

Federation party

When performing a cyber range federation via an operational or a technical federation, there are two or more federation parties, i.e. organisations or part thereof, performing activities of the activities to interconnect cyber ranges or share technical or operational of a cyber exercise or a scenario run in an exercise.

Information and Communication Technology (ICT)

I

Information and communication technology (ICT) covers all the technologies that, combined, allow people and organisations to interact in the digital world.

Live cyber exercise

L

A live cyber exercise is a cyber exercise that is based on real events to increase the realism on selected scenario(s). The exercise includes an active adversary team (Red Team) that conducts an objective campaign against the exercise training audience. Live exercices often include multiple organizations (i.e. the client, its service providers, subcontractors, internal and external partners) who depend on each other for providing business services.

Live cyber range

A live cyber range is a cyber range which is constantly running, i.e. not powered-off between exercises or training sessions. The need for a live environment may be due an internal requirement for the realism of the environment, which contains realistic Internet infrastructures, and simulated common public Internet services, operated or consumed by software automated (ro)bots.

Operational Federation

O

The operational federation of cyber ranges enables parties, e.g. cyber range operators, cyber exercise or cyber range training and planning organizations, to share and exchange scenarios, and technical information of exercises or training environment data in machine readable format. It does not imply integration, which instead requires that two or more cyber ranges must be able to communicate with one another in order to deliver a scenario. Please note: this text has been adopted from (ECSO, 2020) where it was defined simply as Federation and here it is refined to Operational Federation.

Operational Technology

Operational technology (OT) monitors and manages industrial process assets and manufacturing/industrial equipment. It is the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

Overlay Network

An overlay network is a computer network that is built on top of another network.

Red Team

R

The red team is a skilled and organized group acting as adversaries and enemies (threat actors). The red team plans and carries out attacks that the blue team(s) are asked to defend.

Scenario

S

According to (European Cyber Security Organization (ECSO) 2020) a scenario is the content that is used on a cyber range. A scenario may contain only a virtual environment for users to interact with or it may also include a storyline with specific objectives, and some practical or theoretical challenges, or various types of questions. According to (Karjalainen, Kokkonen and Puuska 2019), a scenario ina cyber security exercise is bounded by the simulation environment, contains many Operations, which contain many Events, which contain many Injects. The scenarios are derived from the cyber exercice's goals In this report the referred viewpoint is mentioned, as there are interviews which may reflect either one definition or the other.

SD-WAN

Sofware-defined networking (SDN) in a wide area network (WAN) can be perceived as set of virtualized, software controlled networks.

SD-WAN Orchestrator

The SD-WAN Orchestrator is used for provisioning customers to the network.

SD-WAN Portal

The SD-WAN Portal is used for configuring and managing SD-WAN networks.

Technical Federation

T

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. Once the technical federation is established, the usage of the resources or services may happen seamlessly, i.e. transparently from end user perspective. It may require contracts or other kinds of a trust relationship where the parties agree e.g. acceptable usage of provided functionalities or services. It does not mean that two or more federated data center services are connected together, i.e. they are not integrated.

Testbed

A testbed is a platform for testing (new) technology(ies) using rigorous, transparent, and replicable methods.

Use Scenario

U

A use scenario describes, on abstract level, an end user access or use the product, in this document the technically federated cyber ranges.

Part A: Report on Existing Cyber Ranges

Executive Summary

Part A introduces the conducted survey of existing cyber ranges and the results thereof. The respondents to the survey were volunteering individuals who provided information about the capabilities of the cyber range they work with, experiences in using the range for their needs, and their views on the federation of cyber ranges

The respondents of the survey were selected by approaching through various communication channels[1]. The knowledge and contacts in the area, including close cooperation with ECSO, helped to target the right audience, reach, and get responses from partners that may not be willing to respond to other surveys.

A typical respondent of the survey comes from a large organization from Europe, with 500 or more employees. The respondents represent cyber range providers, operators, or consultants, who actively use a self-hosted or self-operated cyber range. According to the results of the survey, most of the cyber ranges are developed, customized, and operated by less than 10 experts who spend a few days configuring the cyber range for a specific use case. The primary use case of a typical European cyber range is the security education of persons from companies and enterprises, government organizations, and universities. The ranges provide an environment simulating or emulating general critical infrastructure in a single training session for less than 30 learners. The learners access the range remotely and get an individual performance report after the training session. The session lasts up to one day. The technical capabilities of the ranges vary. The only common capabilities are single-sign-on or centralized user management and the number of available virtual machines ranging from tens to thousands.

The hypothesis was that large organisations have the most resources to operate cyber ranges. The survey strengthen the hypothesis. However, there were organisation(s) having less than 249 employees, which were noticeably well resourced. Given the small number of respondents (N=39), more research is required.

Based on the survey and its results, use cases for cyber range technical federation were identified. They are documented in Part B of this deliverable. The Part B also contains production level requirement specification for cyber range technical federation.

[1] The CyberSec4Europe network, social media channels and searching the Internet for cyber range providers and contacting them via email.

1 Introduction to the Report on Existing Cyber Ranges

The purpose of this report is to support CyberSec4Europe project's goals to research and develop European (Master's level) cyber security education and training, collaboration with cyber ranges. This report achieves these goals by:

- listing use-cases, primary target groups, and technical information of existing cyber ranges and of those under construction;
- proposing more fine-grained terminology for cyber range federation;

Part A of this report covers existing cyber ranges and their capabilities, but cyber ranges, which were under planning, are also reported. Even though, the initial assignment was to gather information regarding cyber ranges located in the European geographical area, the task force kept the research survey open for global respondents as well.

1.1 CS4E Cyber Ranges and Capabilities

A cyber range is analogous to a shooting range or a firing range. These ranges can vary in the capacity of the simultaneous training individual users, or exercising troops they can support. In addition, they vary in capability, and in which kind of trainings or exercises can be conducted. Some ranges are intended for archers only, some are suitable for complex and sophisticated weapon systems requiring infrastructure and possibly distributed support systems. Similarly to shooting ranges, cyber ranges are either simulated or emulated environments (Yamin, Katt, & Gkioulos, 2019) sharing many similarities of use cases: developing individuals' skills and knowledge, and arranging competitions and exercises for individuals or groups of people from one or more organisations or companies. Cyber ranges may be static during an event, or they may include moving targets, for example simulated live threat actors. The conducted survey results show that they are also used for recruitment, cyber security research and development, security testing and certification purposes.

Specialised Cyber Ranges

Cyber range use cases and the events thereof are enabled or restricted by its capabilities and capacity. They include the technical aspects, such as computing power, memory and disk capacity, network characteristics and topology, available operating systems and applications, and the physical environment. For example, a cyber range or a test lab capable allowing only physical attendance for only a few attendees differs from a remotely accessible range capable simultaneously supporting several distinct events for distinct customers. A highly specialised "small" cyber range can cope even with modest capacity and capability, but large and realistic environments, which can referred as private clouds, may require considerable investments for the hardware and software licences to provide realistic training or exercise environment for the customers.

When conducting a cyber security competition, training or exercise, multiple cyber ranges can be interconnected. The customers or users of these interconnected cyber ranges may profit from lowered costs (ECSO, 2020) and the availability of purposeful realistic event contents. Karjalainen et al. (Figure 1) have illustrated the process from the planning of a cyber security exercise to its conducting. Derived from their approach, it can be concluded that after setting the exercise goals, one could evaluate which cyber range should be used or which cyber ranges should be interconnected in order to provide an environment which enables the achievement of the goals of an exercise. For the interconnection between cyber ranges, remote accessibility to the cyber ranges are required and characteristics of cyber ranges Internet connection are critical for the end user. Interoperability between cyber ranges can be achieved even if the cyber ranges are offline, i.e. not interconnected.

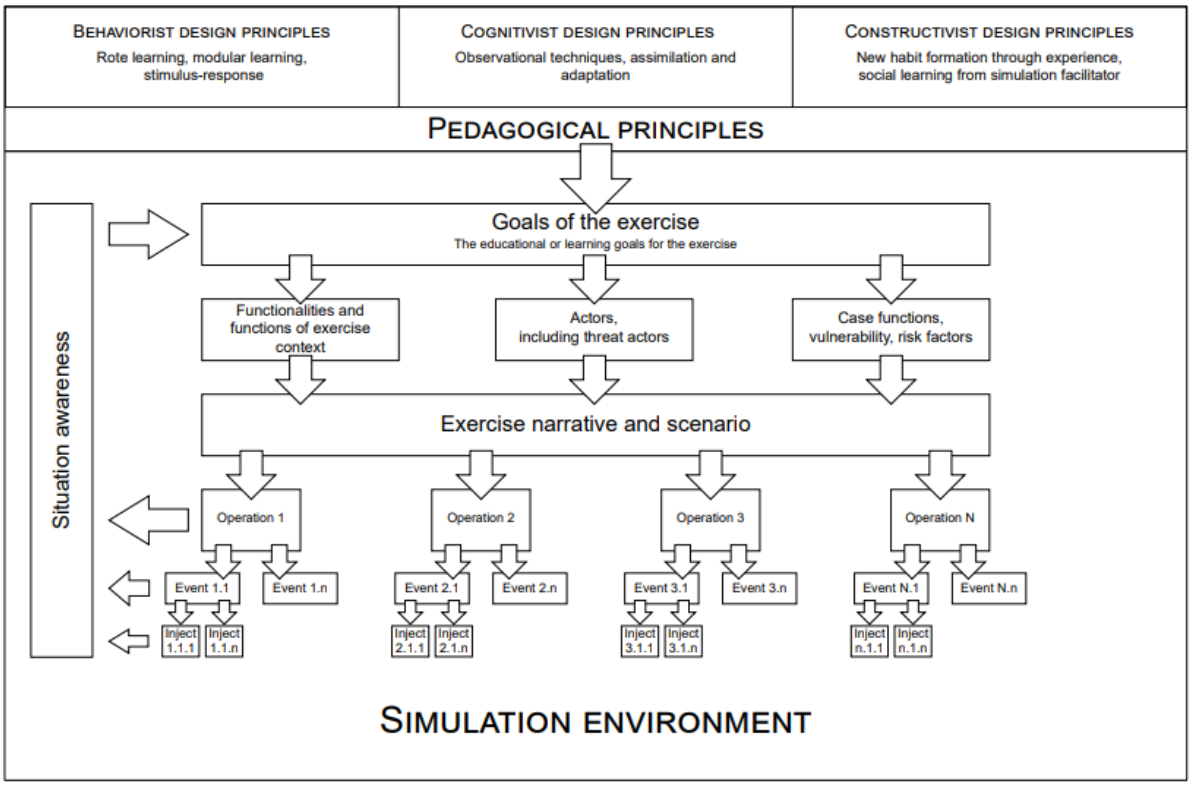

Figure 1: The relationship of the simulation environment with the exercise scenario(s) (Karjalainen, Kokkonen, & Puuska, Pedagogical Aspects of Cyber Security Exercises, 2019).

A Proposal Regarding the Federation of Cyber Ranges

The development and operations of a cyber range may require considerable resources in terms of funding, skilled people and working time. Interconnecting two or more cyber ranges not only offers the participants of a competition, training or exercise a broader or realistic environment for the event, but it also may relieve the required resources for developing or operating a cyber range. For cyber range vendors or operators this possibility also enables them to focus on a limited number of use cases, thus offering more sophisticated environments and services. (ECSO, 2020), (Yamin, Katt, & Gkioulos, 2019)

Technically, the interconnection of various cyber ranges has been called integration or more broadly: federation of cyber ranges. During this work, while developing the survey of existing cyber ranges, discussing within the task force, interviewing selected survey participants, studying peer-reviewed documents, publications and reports, it was becoming evident that the term cyber range federation is not well established. In some occasions, it even conflicted with the established definition of commodity-federated services; depending with whom one was discussing with, or which document was under study, even when the person or author(s) were cyber security or even cyber range specialists or researchers, the interpretation of cyber range federation varied. It varied from sharing scenario data in machine readable format, utilizing or consuming resources from a cyber range cloud-computing-like uses cases, e.g. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), to offering and utilizing specific niche functionalities and features available on a cyber range as part of another cyber range offering, either temporary or until further notice. Having this kind of broad variance causes not only confusion within people in the community and its stakeholders, but also consumes resources. This problem could be avoided. As a solution, we propose a more fine-grained definition for cyber range federation, by introducing two federation aspects: the **Operational Federation** and the **Technical Federation**. Both of these aspects support, in their own way, the fundamental meaning of cyber range federation, which is interoperability between cyber ranges.

ECSO defines cyber range federation as sharing cyber range operational and technical data in machine-readable format (ECSO, 2020):

> *In relation to cyber ranges, standards of operation include scenario description language, description of cyber range capabilities, and request and provision of cyber range services within the federation. With regards to scenarios, for instance, it may be possible to use a common way of describing them across different cyber ranges, allowing each cyber range to implement and deliver them in their own specific way.*

For the definition of **Operational Federation** we propose to follow ECSO current definition *federation of cyber range*, but renaming it. Referring to the ECSO report the operational federation does not imply integration [or interconnection] of cyber ranges. It clearly states that interoperability by exchanging technical and operational data is the value it provides to the federation parties, even if the cyber ranges would not be interconnected.

We propose the term **Technical Federation** of cyber ranges to define the agreement between the federation parties on how they can utilize or consume specified functionalities, services, capabilities or resources from federation parties and implementing them together. The implementation technology of the technical federation is not restricted or instructed, but it is rather a matter of the planning and implementation phase of the activity. The technical federation of the cyber ranges allows the offering of the federated ranges to be simultaneously used from remote locations, even cross-border. Neither the operational federation nor the technical federation require the other one to be implemented or deployed.

By distinguishing which kind of cyber range federation, operational or technical, is being discussed, the participants from the cyber security and cyber range communities, and the stakeholders can easily adapt themselves to the subject and contents, and participate into the discussion. The concepts would, thus, be clear either when sharing operational or technical data without interconnecting cyber ranges, or when explicitly interconnecting cyber ranges targeting to create joint-cyber ranges by federation parties in order to offer enhanced cyber exercises or training. Without the proposed clarification of definitions, we foresee that there will be confusion and blind spots when discussing on interconnecting cyber ranges, as some of them can be considered as being private clouds. The technical federation does not imply that a cyber range should be a private cloud.

The rest of Part A discusses the conducted survey and its results.

2 State of the Art

This chapter presents the implementation of the State of the Art survey, topic definition, purpose of the survey and survey questions. It also presents the target group of the survey, the chosen material collection method and the structure of the questionnaire and the interviews.

2.1 Survey Objectives

The main objective was to study State of the Art of cyber ranges in Europe, and to assess and compare the features, functionalities and services of the cyber ranges. Secondary targets were gather testing and certification requirements from the cybersecurity verticals and requirements and conditions for cyber range federation and implementation.

2.2 Survey Methods

The method is the use of a survey, which provides quantitative data since the survey consisted of multiple choice and check box questions. The survey form is provided in Annex A: Survey form. In this deliverable, the main focus was on the quantitative analysis of the received data.

The survey also included some open-ended questions to gather more information. Moreover, qualitative interviews were made to find more detailed information on the areas of federation and certification requirements. The interview questions were open-ended and the interview was a semi-structured one. The interview questions were provided in advance, but there was also room for new questions and open discussions to be raised during the interview. The remote interviews were recorded with the permission from interviewees and the interviews were transcribed.

2.3 Survey Population and Sampling

The respondents of the survey were selected by approaching through various communication channels[2]. The knowledge and contacts in the area, including close cooperation with ECSO, helped to target the right audience, reach, and get responses from partners that may not be willing to respond to other surveys.

The survey was open for two weeks from 23rd April till 7th May 2020 and within that time 13 responses were received, and, thus, the survey was extended to be open until 27th May 2020. Eventually a total of 44 responses were received.

Qualitative interviews were made for survey respondents who answered yes to survey questions *32 "Have you done cyber range federation or integration?"* and *37 "Below are my business contact details, which I want to voluntary provide for interview purposes"*. Four respondents matched these criteria and they were contacted for further interviews. An interview with three of these four respondents was organised, while one respondent could not schedule the interview because of the summer break. The interview questions (Annex B: Interview questions) were provided in advance to the respondents so that they were able to prepare themselves. The interview had mandatory questions, and questions that were asked if the agreed interview time limit allowed.

The survey was open to cyber range providers, operators and consultants, and to cyber range users. The users were included to acquire more understanding of the use of cyber ranges.

2.4 Survey Questions

The main objective was to study State of the Art of cyber ranges in Europe, and to assess and compare the features, functionalities and services of the cyber ranges.

The survey questions were selected to identify the use cases of cyber ranges, the roles of the participants, and the capabilities and the capacity of cyber range vendors and operators as well as the characteristics of environments used by individuals, companies or organisations.

The question types were: multiple choice, check box and open text field. The survey questions are categorized in this report under the following themes:

- organization background (Q1 – Q4),
- cyber range background (Q5 – Q18),
- cyber range performance (Q19 – Q20),

[2] The CyberSec4Europe network, social media channels and searching the Internet for cyber range providers and contacting them via email.

- cyber range technical specification (Q21 – Q31),
- cyber range federation (Q32 – Q33) and
- cyber range connectivity (Q34 – Q36).

A more detailed description of each theme is provided below.

2.4.1 The Survey Questions

Respondent Organization background (Q1 – Q4)

This section provides answers to the question "what kind of organizations responded to the survey". This category provides basic background information about the respondent´s organization in terms of number of personnel working in the organization, the country (of the headquarters) in which the organization operates from, what is the role of the cyber range is in this specific organization, and the current status of using cyber ranges in the organization.

It has been well analysed, for example in (ECSO, 2020), and (Yamin, Katt, & Gkioulos, 2019), that developing a large cyber range requires considerable resources, in terms of funding, skilled persons and work time. Our hypothesis is that operating a cyber range follows that: large cyber ranges require more work and more people that are skilled. In this theme, the size of the organisation is measured through the number of its employees.

Cyber range background (Q5 – Q18)

This section provides answers to the question "what kind of cyber ranges do the respondent organizations have or plan to acquire". This category provides information on the background of the cyber ranges, how much personnel is involved in the organization´s cyber range operations as well as how much effort is needed to configure the cyber range for a specific use case. This category also highlights the characteristics of the cyber range and opens up the primary use cases, target groups and participant roles as well as some basic technical aspects of the cyber range in order to form an image of the environment in question. Where seen relevant, the responses are correlated with the organisation size.

Alternatives of hosting and operating a cyber range have expanded due to the advancement in the public cloud services, technology stacks offering capability to establish public or private clouds by an organisation or a company, in addition to lab and class based solutions. In addition, there are commercial cyber range vendors offering services offering various business models. This theme determines various hosting and operating types of cyber ranges that is then correlated with the organisation size.

Performance reports of cyber range attendees (Q19 – Q20)

This section provides answers to the performance of the cyber range in question. This category deepens into the cyber ranges in terms of providing information on performance reports and durations of individual training sessions.

Cyber range technical specification (Q21 – Q31)

This section provides answers to the capabilities of cyber ranges in terms of their technical specifications. This category deepens the view of the technical choices of the specific cyber range.

The technical specifications should strengthen the assumption that cyber ranges requiring a large amount of computing power, storage, and services to operate are developed and operated most likely by large organisations rather than by small ones.

There is no established definition for the cyber range size or for the categorization of how realistic is a cyber range, which would cover at least the capabilities, capacity, features, functions or services per se, or relatively to a use case. For example, a dedicated cyber range, with a limited number of technical

parameters or features, and using (commercial) public services may be very realistic and may cover most of the (domain- specific) use cases. However, as it would be limited by nature, it might not be considered as a large environment. This, however, is speculative, as there is no established taxonomy. There is a need to further discuss some of the aspects which could be used in determining whether a cyber range is realistic or not, but this needs further discussion and research.

Cyber range federation (Q32 – Q33)

This section provides answers to whether any interconnections (federation or integration) of the cyber ranges has been done or is planned to be done. In other words, this category gives views on the implementation and plans for implementing interconnections of cyber ranges with one or more other environment(s) and the cross-use of each other´s services via this federation in a joint event or exercise.

During the survey, no definition of federation was given to the respondents. Elsewhere in Part A of this document a fine-grained definition for cyber range federation is discussed and proposed.

Cyber range connectivity (Q34 – Q36)

This section provides answers to the connectivity of the cyber range. This category gives further information on the cyber range´s Internet connectivity, whether it is dedicated or not, and details on the connectivity speed and latency (Round-Trip-Time).

The cyber range's connectivity to the Internet is critical to interconnect cyber ranges, especially when planning and implementing a technical federation of two or more cyber ranges. The characteristics of the connectivity are important for the experience of the end-users who use interconnected cyber ranges.

2.4.2 The Interview Questions

The qualitative interviews included questions on the areas of cyber range federation in terms of use cases, benefits, and specification of what is meant with the term federation and the requirements of federation. There were also two questions on certification requirements for cyber ranges. The interview questions were open-ended.

3 Survey Results

Five respondents were taken out of the analysis. Four of these were considered as irrelevant (almost empty) and one respondent had answered only to question 3: *Role of cyber range in our organization*: "Is not used nor planned". Since the research focuses on cyber range providers that are using or planning to use the cyber range this respondent was left out of the analysis. Altogether 39 respondents were taken into account and from these altogether 23 respondents were in the position of answering the technical questions related to the cyber range. There were no mandatory questions in the survey and, therefore, the number of respondents in each specific question varied. This is represented as N in the survey results. The results in figures and tables are shown in absolute numbers instead of percentage due the limited amount of responses received.

Cyber range phase	Organisation In EU	Other countries	Total
Is planning	13	0	**13**
Is using	21	5	**26**
TOTAL	**34**	**5**	**39**

Table 1: Division of final survey answers by using cyber ranges and planning to use cyber ranges (N=39).

Table 1 shows the final survey respondents categorized to the ones using cyber ranges and the ones planning to use cyber ranges divided into EU, other countries and total.

3.1 Organization Background

This category provides basic background information about the respondent´s organization in terms of headcount, the country (of headquarters) in which the organization operates, what the role of the cyber range is in this specific organization and the current status of using cyber ranges in the organization.

Name of cyber range	Cyber range operator or vendor	Site
Airbus CyberRange	Airbus CyberSecurity	https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/ (Ed. note)
AIT Cyber Range	AIT Austrian Institute of Technology	https://cyberrange.at/
Cisco Cyber Range	Cisco	https://cisco.com
Cloud Range	Cloud Range	https://www.cloudrangecyber.com
CRATE - Cyber range and training environment	The Swedish Defence Research Agency (FOI)	https://www.foi.se/crate
Cyber Czech	NUKIB	https://www.kypo.cz/en (Ed. note)
Cyber Integration, Test and Evaluation Framework (CITEF)	RHEA	https://www.rheagroup.com/cyber-range (Ed. note)
Cyber Range	Field Effect	https://fieldeffect.com/blog/what-is-a-cyber-range/ (Ed. note)
Cyber Test Lab	Nutanix	https://cybertestlab.turkuamk.fi/
Cyberbit Range	Cyberbit	https://www.cyberbit.com
Cyber-MAR cyber range	more than one vendors	https://www.cyber-mar.eu
Dependable Systems CyberLabs	Tampere Universities	https://sites.tuni.fi/dependablesystems/cyberlabs/
Diateam HNS	Diateam	https://diateam.com
E-FCR	ECHO pilot	https://echonetwork.eu/echo-federated-cyber-range/ (Ed. note)
Equipment to generate realistic	Rugged Tooling	https://ruggedtooling.com/ruge-ip-load-generator/ (Ed. note)

Name of cyber range	Cyber range operator or vendor	Site
traffic for cyber ranges & monitor the traffic during exercise		
Estonian Defence Forces Cyber Range	Estonian Defence Forces / CR14	https://mil.ee/en/landforces/cyber-command/ (Ed. note)
Instance Lab	Information not provided	https://www.cynic.se/training/instance-lab/ (Ed. note)
KTH Ethical Hacking Cyber Range	KTH	https://www.kth.se/nse/studies/online-course-in-ethical-hacking-7-5-hp/course-information-1.819016 (Ed. note)
KYPO Cyber Range Platform	Masaryk University	https://www.kypo.cz/en
Portable Cyber Range	GT Cyber Technologies	https://cyber.guardtime.com/services (Ed. note)
Realistic Global Cyber Environment (RGCE)	JYVSECTEC	https://jyvsectec.fi
ROOM#42	SMILE	https://www.room42.lu/ (Ed. note)
THREAT-ARREST	EU funded project, Consortium with 15 members, the coordinator is FORTH	https://www.threat-arrest.eu/
VTT Cyber Range	VTT	https://www.vttresearch.com/en/ourservices/cyber-security (Ed. note)

Table 2: Name of cyber range, operator and Internet address.

Table 2 shows the names of the cyber ranges of the survey respondents, the name of the operator and the Internet address. In case the Internet address was not provided, but it could be found online by the researchers, it was included in the field. As seen from the answers there were institutional, military and commercial cyber ranges.

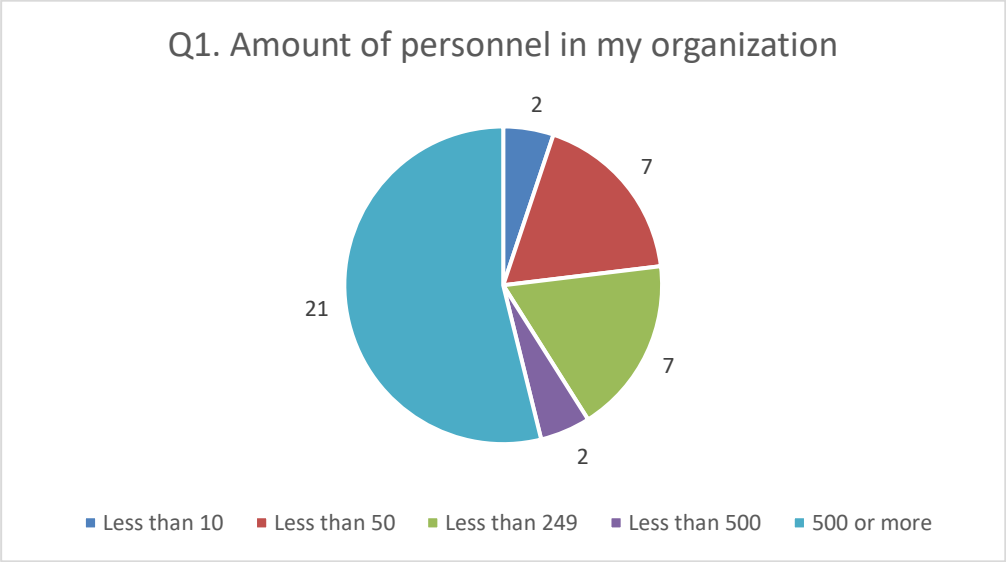

Figure 2: Distribution of responses regarding the size of the personnel in the respondents' organization (N=39).

Figure 2 shows that 21 respondents (54%) were from organizations with 500 or more employees. Two respondents (5%) were from an organization with less than 500 employees (249-499 employees). Seven respondents (18%) were from an organization with less than 249 employees (50-248 employees). Also seven respondents (18%) were from an organization with less than 50 employees (10-49 employees). Two respondents (5%) were from an organization with less than 10 employees.

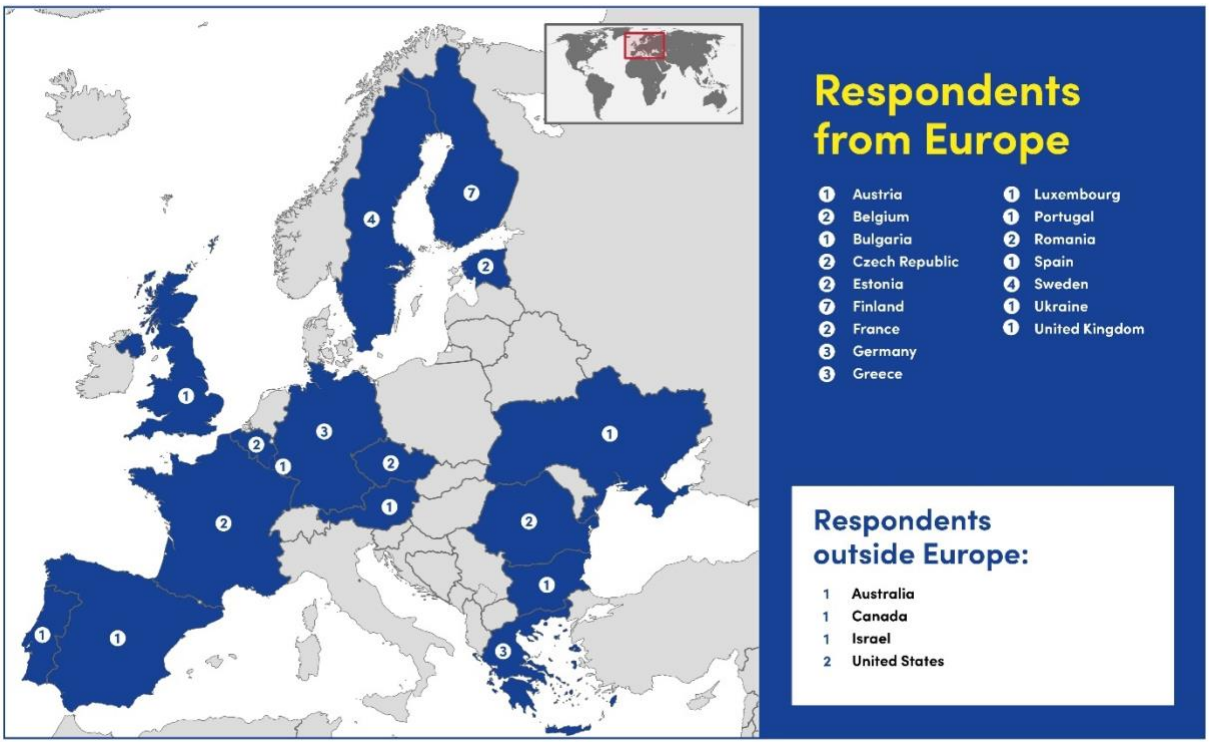

Figure 3: Country of organization's HQ (Q2).

The survey respondents were spread quite evenly across Europe (see Figure 3) with participants from Northern (14), Southern (5), Eastern (6) and Western Europe (9). Five respondents were from outside Europe: one from Australia, one from Canada, one from Israel and two from the United States.

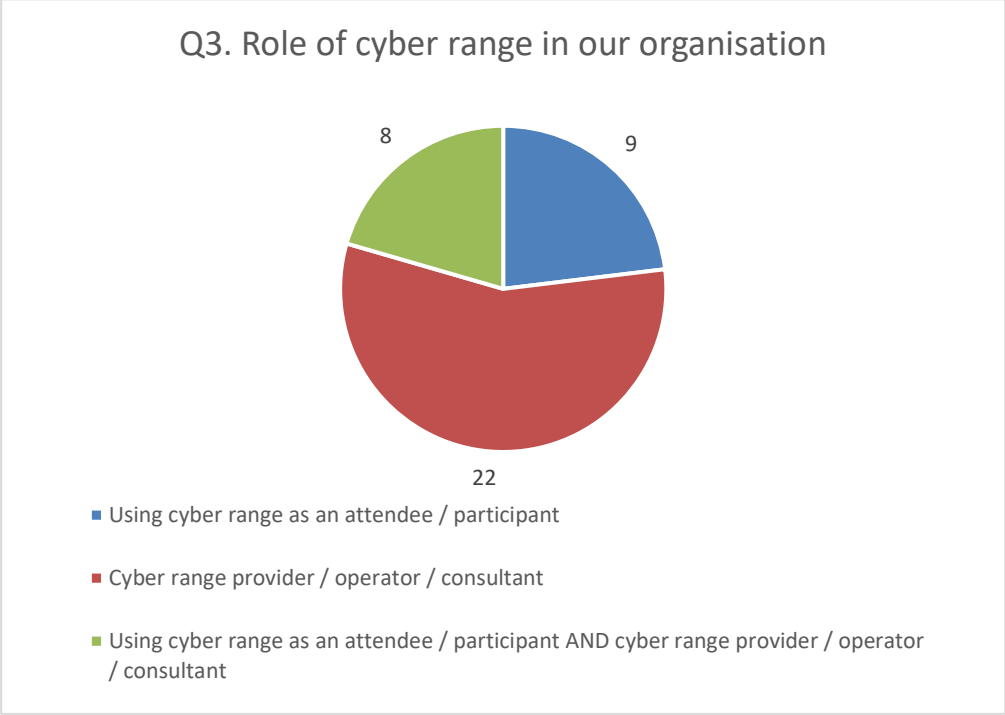

Figure 4: Role of cyber range in our organization (N=39).

As shown in Figure 4, 22 (56%) of respondents, stated that their organization is a cyber range provider, operator or consultant. Nine (23%) stated that they are using cyber range as an attendee or as a participant. Eight (21%) stated that both of the options match their organization; they are a cyber range provider, operator or consultant and use a cyber range as an attendee or participant.

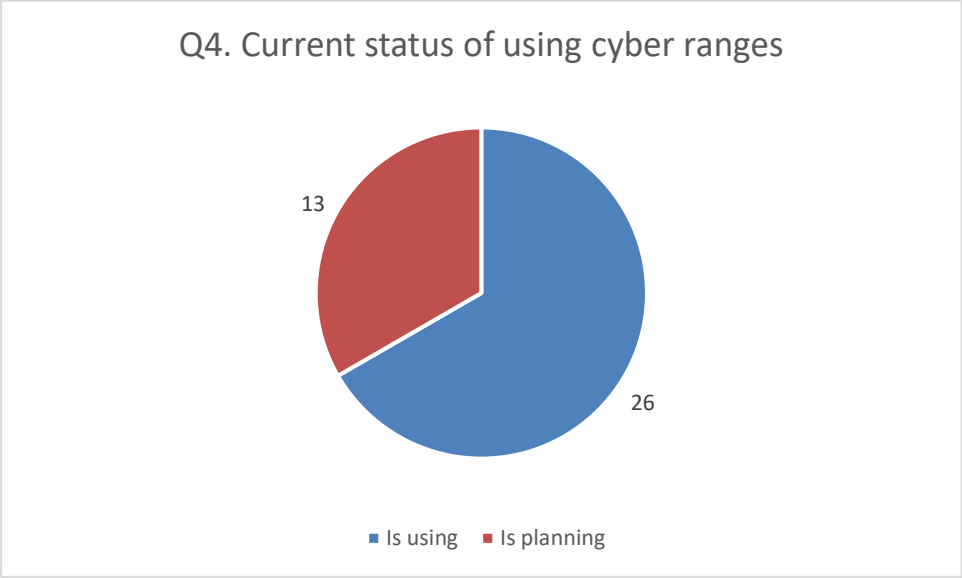

Figure 5: Current status of using cyber ranges (N=39).

As Figure 5 shows, 26 respondents (67%) answered that they are currently using cyber ranges and 13 respondents (33%) answered that they are planning to use cyber ranges.

Organization size	Is Using	Q4. Current status of using cyber ranges		
		Attendee / participant	Cyber range provider / operator / consultant	Using as both
500 or more	17	2	9	6
Less than 500	2	1	1	0
Less than 249	4	0	4	0
Less than 50	3	1	2	0
Total	26	4	16	6

Table 3: Comparison of the current role of organisations using cyber range with the number of employees (N=26).

Focusing on the current users and providers of cyber ranges, Table 3 shows that organisations having 500 or more employees were the most frequently reported to be using a cyber range – with 17 (65%) of all responses. From these organisations, 9 (53%) were only offering services, 6 (35%) or offering services and using cyber ranges, two (12%) were only using cyber ranges. Organisations with less than 500 persons reported two (8%) responses, and the responses were split with equal share between attendee or participant, and providing cyber ranges or cyber range services as operator or consultant. Four (15%) respondents were from organisations with less than 249 employees, and all of them were providing cyber ranges or cyber range services as operator or consultant. Three (12%) respondents were from organisations with less than 50 employees, one (33%) of those as attendee or participant in a cyber range, and two (67%) as cyber range vendor, operator or consultant. Organisations having less than 10 employees did not report current use related to cyber ranges.

An interesting discovery from this data is that very rarely organisations were both offering services and using a cyber range. This could mean that the organisations offering cyber range services or cyber ranges provide services or ranges, which they cannot utilize themselves, or they simply have not done that yet.

Organization size	Is planning	Q4. Planned status of using cyber ranges		
		An attendee / participant	Cyber range provider / operator / consultant	Using as both
500 or more	4	0	3	1
Less than 500	0	0	0	0
Less than 249	3	2	0	1
Less than 50	4	2	2	0
Less than 10	2	1	1	0
Total	13	5	6	2

Table 4: Comparison of planned role of cyber range in an organisation with the number of employees (N=13).

The future plans for cyber ranges in organisations compared to the size of the organisation (Table 4) shows that there might be new cyber range providers or service providers available in the future, as new participants.

Four (31%) respondents from organisation with 500 or more employees were planning to enter to cyber range services. Three (75%) of these were focusing offering cyber ranges or provider related services, and one (25%) offering services and using cyber ranges themselves. Three (23%) organisations with less than 249 employees had plans, two (67%) of them as using cyber ranges as attendees or participants, and one (33%) as offering cyber ranges or related services and attending themselves to events in cyber ranges. Four (31%) organisations having less than 50 employees had plans, splitting with equal share of two (50%) responses to attending or participating to a cyber range event, and offering cyber ranges or related services.

Two (15%) organisations having less than 10 employees were planning, one to use as an attendee or one to provide cyber ranges or related services. This is a change from reported current users or providers shown previously in Table 3, as there were no organisations of this size doing anything related to cyber ranges. Organisations with less than 500 employees had no plans regarding cyber ranges.

Again, for some reason majority of the providers of cyber ranges or related services were not planning to use cyber ranges themselves, as only two (25%) were planning to provide cyber ranges or related services and use ranges themselves.

The results indicate that the number of cyber ranges attendees or participants is on the rise. Currently, there were four organisations purely attending to some cyber range-based events, but the plans show that five more organisations have plans to do the same, equalling a 125% increase. The results also show that large organisations, where the number employees was 500 or more, represents the majority of all the respondents which were offering cyber ranges, operating them or planning to do so.

3.2 Cyber Range Background

This category provides information on the background of the cyber ranges, how many people are involved in the organisation´s cyber range operations as well as how much effort is needed to configure a cyber range for a specific use case. This category also highlights the characteristics of the cyber ranges and opens up the primary use cases, target groups and participant roles as well as some basic technical aspects of the cyber ranges in order to form an image of the environment in question. The number of

respondents for this question is 39, but some of the respondents selected two or all of the options since there was no limitation on selecting several options.

Question 5 gives an answer to the hosting type of the cyber range. The question was a multiple-choice question with three options and the option to enter a free-text hosting type.

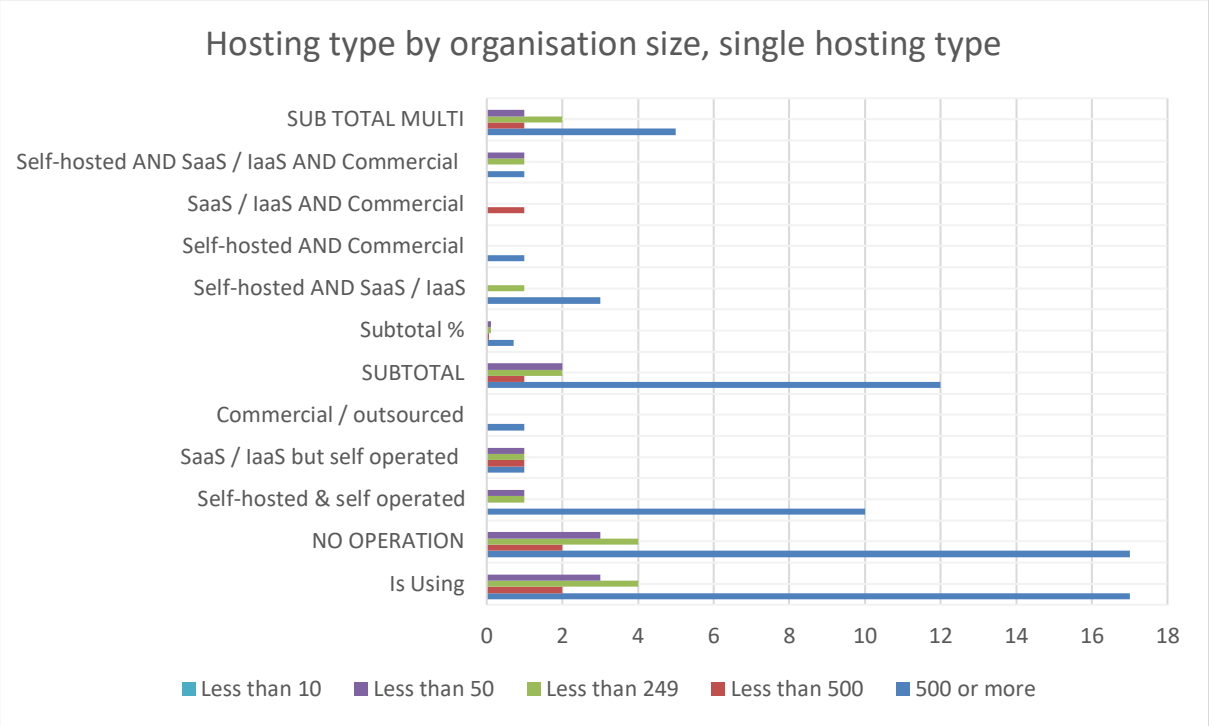

Figure 6: Hosting type by organisation size, single hosting type (N=17).

The current single hosting type of existing cyber range operators and users (Figure 6) shows that 12 (71%) of respondents were from organisations having 500 or more employees. They selected 10 (83%) times self-hosted and self-operated, and once (8%) were selected both SaaS / IaaS but self-operated and Commercial / outsourced options. Organisations with less than 500 employees had a single (6%) hosting type, SaaS / IaaS but self-operated. Organisations having less than 249 employees had two (12%) single hosting type environments, one Self-hosted and self-operated, and one SaaS / IaaS but self-operated, which was also the case for two (12%) of organisations with less than 50 employees.

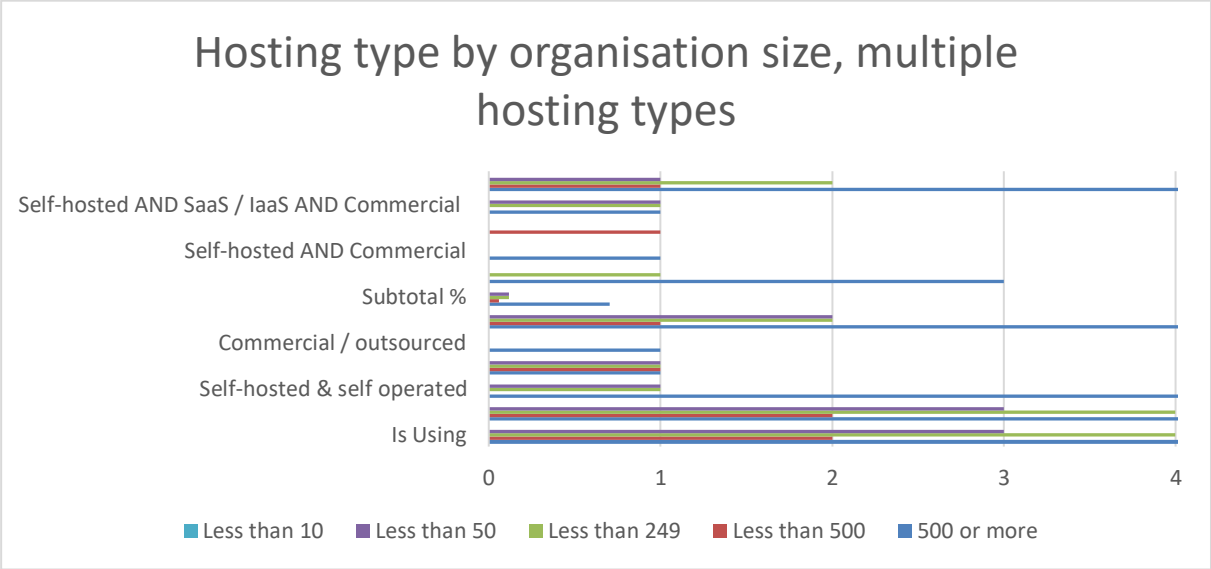

Figure 7: Hosting type by organisation size, multiple hosting types (N=9).

The distribution of multiple hosting types by organisation size is shown in Figure 7. The most selected combination was self-hosted and self-operated, and SaaS / IaaS but self-operated with four (44%) selections, selected by three (75%) organisations with 500 or more and once (25%) by an organisation with less than 249 employees. The combination of all three possible hosting types, self-hosted and SaaS / IaaS and commercial was selected by three (33%) organisations, split with equal share to organisations with 500 or more, organisations with less than 249 and organisations with less than 50 employees. The combination of SaaS / IaaS and commercial was selected once (11%) by an organisation with less than 500 employees. The combination of self-hosted and commercial was selected once (11%) by and organisation with 500 or more employees.

The results confirm that large organisations run cyber ranges by themselves, only rarely needing commercial or external platforms, while smaller organisations use external vendors or partners for hosting or operating a cyber range. When using multiple hosting types whilst offering a cyber range, it may give benefit to the users, as they are potentially receiving more or more realistic use cases. The survey's SaaS / IaaS option are considered to be part of cloud computing services. The Commercial or outsourced option is not that clear, as the survey does not go into further details beyond the hosting type.

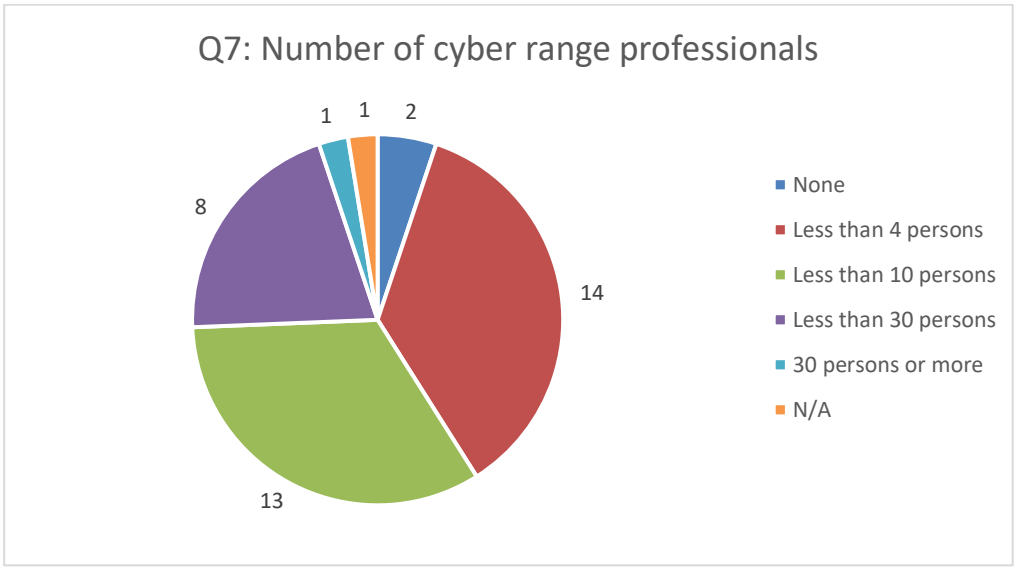

Figure 8: Number of cyber range professionals (N=39).

The hypothesis was that in large organisations (500 or more employees) have more cyber range professionals to perform the administrative tasks on the cyber range and they also perform the necessary use-case based customisations to it, and do cyber exercises or training planning, and execution.

The numbers of cyber range professionals are shown in Figure 8. 16 respondents (41%) answered that they have less than 4 cyber range exercise professionals working in the organization, 13 respondents (33%) had less than 10 persons, four respondents (10%) less than 30 person and four respondents (10%) did not have any cyber range professionals. In one organisation there were 30 professionals or more while one respondent did not give an answer to this question (N/A).

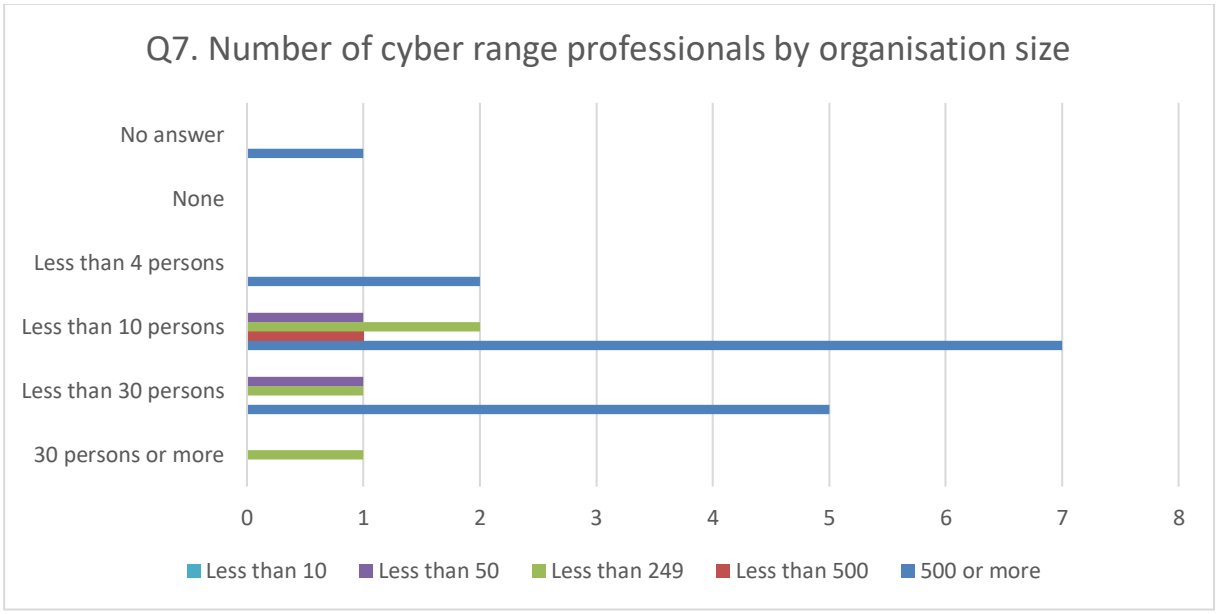

Figure 9: Number of cyber range professionals by organisation size (N=22).

The number of cyber range professionals correlated with organisation size and listing only filtered by current cyber range vendors or service providers is shown in Figure 9. Having 30 or more cyber range professionals was reported by only one (5%) respondent, the organisation having less than 249 employees. Less than 30 professionals were selected by seven (32%) respondents. It splits to five (71%) organisations with 500 or more employees, one (14%) organisation with less than 249 and one (14%) organisation less than 50 employees. Less than 10 cyber range professionals was total in 11 (50%) of responses. Seven (64%) of these respondents were from an organisation having 500 or more employees, one (9%) having less than 500, two (18%) having less than 249, and one (9%) respondent having less than 50 employees. Most of the cyber range providers or cyber range service providers have less than 30 cyber range professionals. Only one reported having 30 or more professionals and perhaps surprisingly it was reported by an organisation having less than 249 employees. Our assumption was that large companies have the most resources to operate cyber ranges. The results of this question strengthen the assumption.

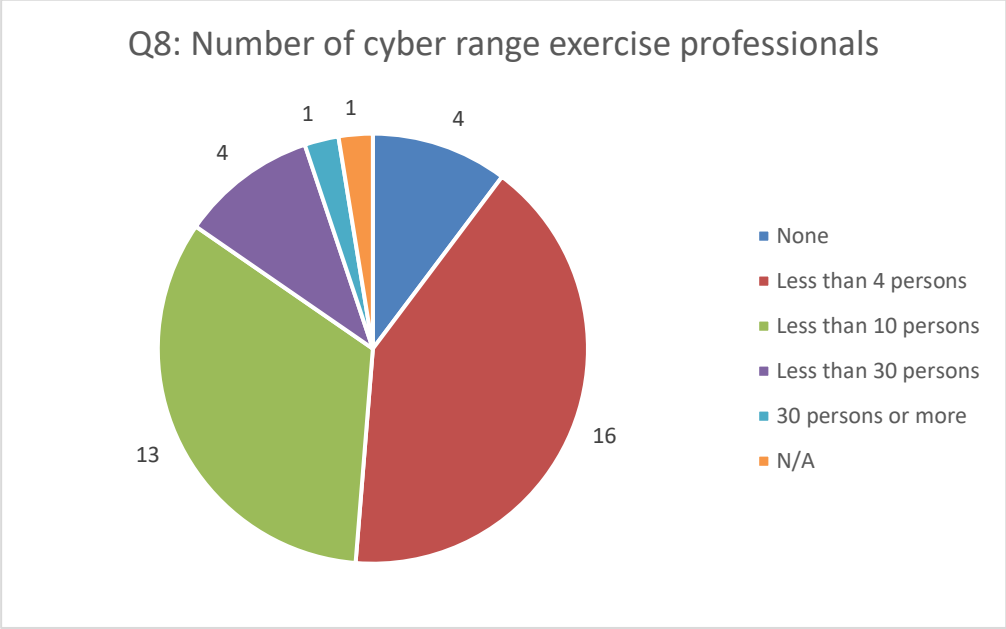

Figure 10: Number of cyber range exercise professionals (N=39).

The number of cyber range exercise professionals are shown in Figure 10. 16 (41%) answered that they have less than 4 cyber range exercise professionals working in the organization, 13 (33%) had less than 10 professionals, four (10%) less than 30 professionals and also four (10%) did not have any cyber range professionals. In one organization there were 30 persons or more professionals and one respondent did not give an answer to this question (N/A).

The number of cyber exercise professionals correlated with the number organisation size so close to the number of cyber range professionals, so it has been left out as a figure of its own. Again, only one reported having 30 or more cyber exercise professionals, and it was from an organisation having less than 249 employees.

These results amplify the assumption that large organisations have the most resources, in this case the number of cyber range and cyber exercise professionals to provide and operate a cyber range and related services.

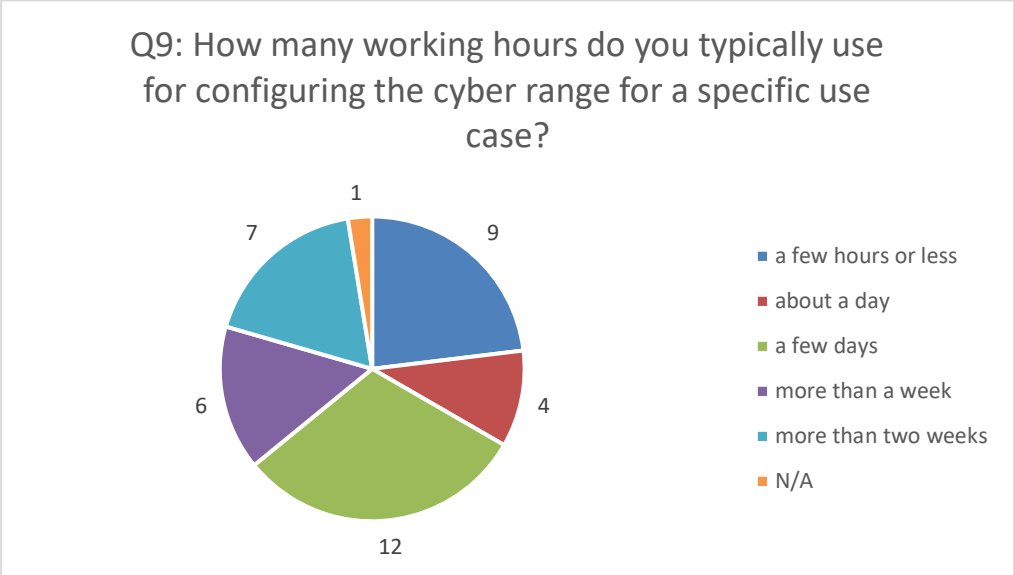

Figure 11: How many working hours do you typically use for configuring the cyber range for a specific use case? (N=39).

Figure 11 shows how many working hours are typically used for configuring the cyber range for a specific use case. 12 respondents (31%) answered that configuring the cyber range takes typically a few days. Nine respondents (23%) answered that it takes a few hours or less, seven respondents (18%) more than two weeks, six respondents (15%) more than a week, four respondents (10%) answered about a day and one respondent did not answer the question (N/A).

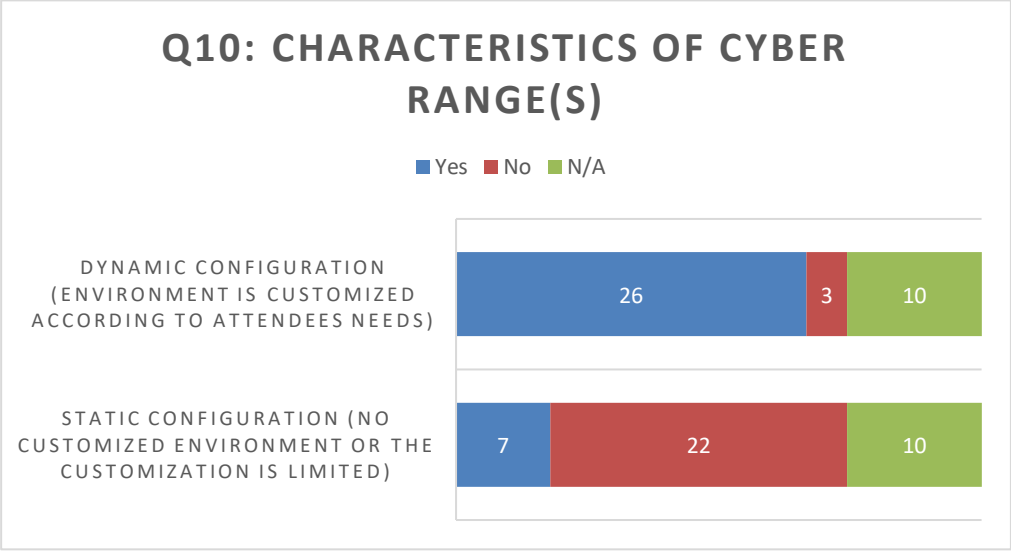

Figure 12: Characteristics of cyber range(s) (N=29).

The characteristics of a cyber range may need to be adapted according to the use case of the event, so that it adapts to changing (customer) requirements, for example bringing new simulated companies and their available IT/OT networks. The characteristics of the cyber range(s) are shown in Figure 12. This was a multiple-choice question with two options. Since this question was only targeted to respondents that selected “Cyber range provider/operator/consultant” as the answer to Question 3 “Role of cyber

range in our organisation", ten respondents were categorised as N/A in the graph. Only 29 respondents answered this question and four of those selected both options (dynamic and static configuration). 26 respondents answered that the cyber range is configured dynamically so that the environment is customized according to the attendees needs and seven respondents answered that the cyber range has a static configuration so there is no possibility for customizing the environment or the customization possibilities are limited. Both of these numbers include the four respondents that chose both options.

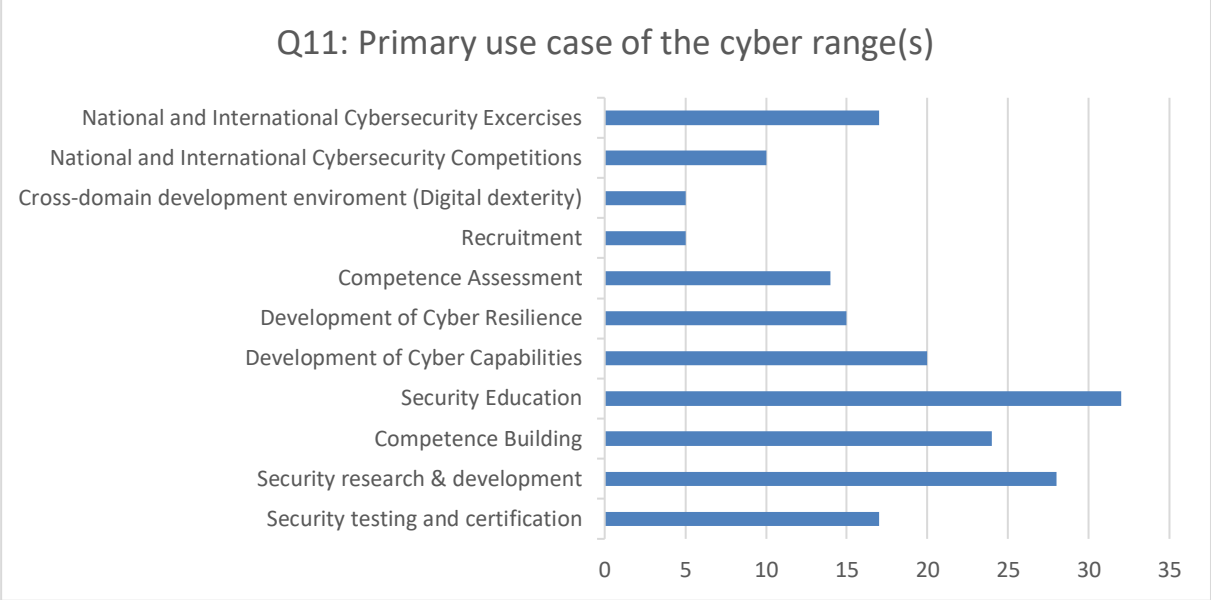

Figure 13: Primary use cases of the cyber range(s) (N=39).

The primary use cases of the cyber range(s) are shown in Figure 13. This was a multiple-choice question with 11 different options that are listed in the figure above. Two respondents selected all options as primary use cases. Six respondents chose only one primary use case. The top three use cases were: security education (32), security research and development (28) and competence building (24).

As mentioned earlier, only rare cyber range providers, operators or consultants used a cyber range themselves. However, they could benefit utilizing it for example in recruitment, developing the cyber resilience of their own organisation and business, and testing their products or (digital) services in a cyber range.

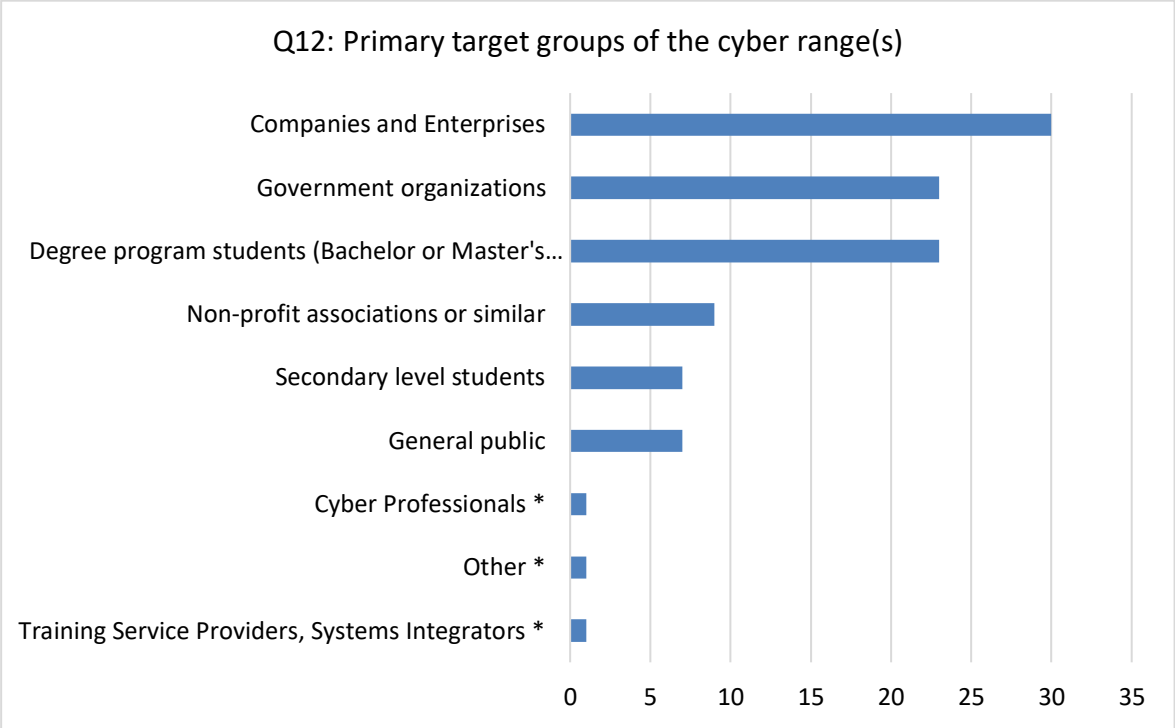

Figure 14: Primary target groups of the cyber range(s) (N=39).

The primary target groups of the cyber range(s) are shown in Figure 14. This was a multiple-choice question with six pre-defined options and an "Other" option. 30 respondents selected more than one option. There was an open text field to describe the other roles and the answers have been included in the figure, marked with an asterisk.

Target groups in descending order were:

- Companies and enterprises (30)
- Government organizations (23)
- Degree program students (Bachelor, or Master's degree students) (23)
- Non-profit associations or similar (9)
- Secondary level students (7)
- General public (7)
- Cyber Professionals* (1)
- Other * (1)
- Training Service Providers, Systems Integrators * (1)

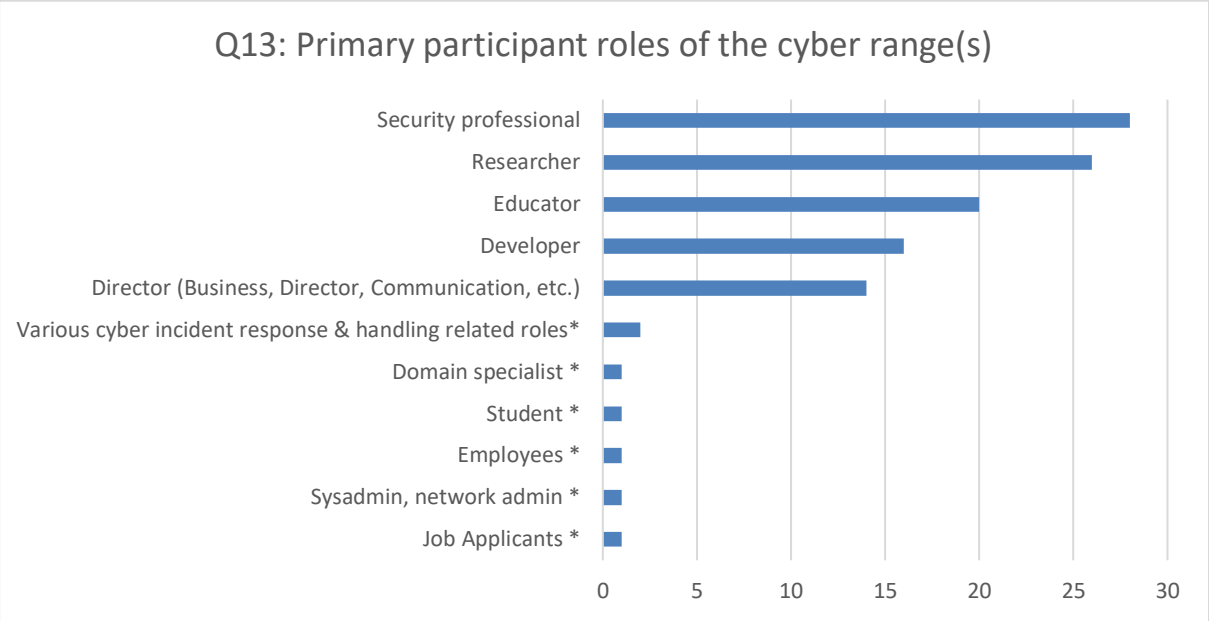

Figure 15: Primary participant roles of the cyber range(s) (N=38).

The primary participant roles of the cyber range(s) are shown in Figure 15. This was a multiple-choice question with five options and an "Other" option. 30 of the 38 respondents selected more than one option. There was an open text field to describe the other roles and the answers have been included in the figure, marked with an asterisk. The participant roles in descending order were:

- Security professional (28)
- Researcher (26)
- Educator (20)
- Developer (16)
- Director (Business Director, Communications, etc.) (14)
- Various cyber incident response and handing related roles * (2)
- Domain specialist * (1)
- Student * (1)
- Employees * (1)
- System administrators, network administrators * (1)
- Job applicants * (1)

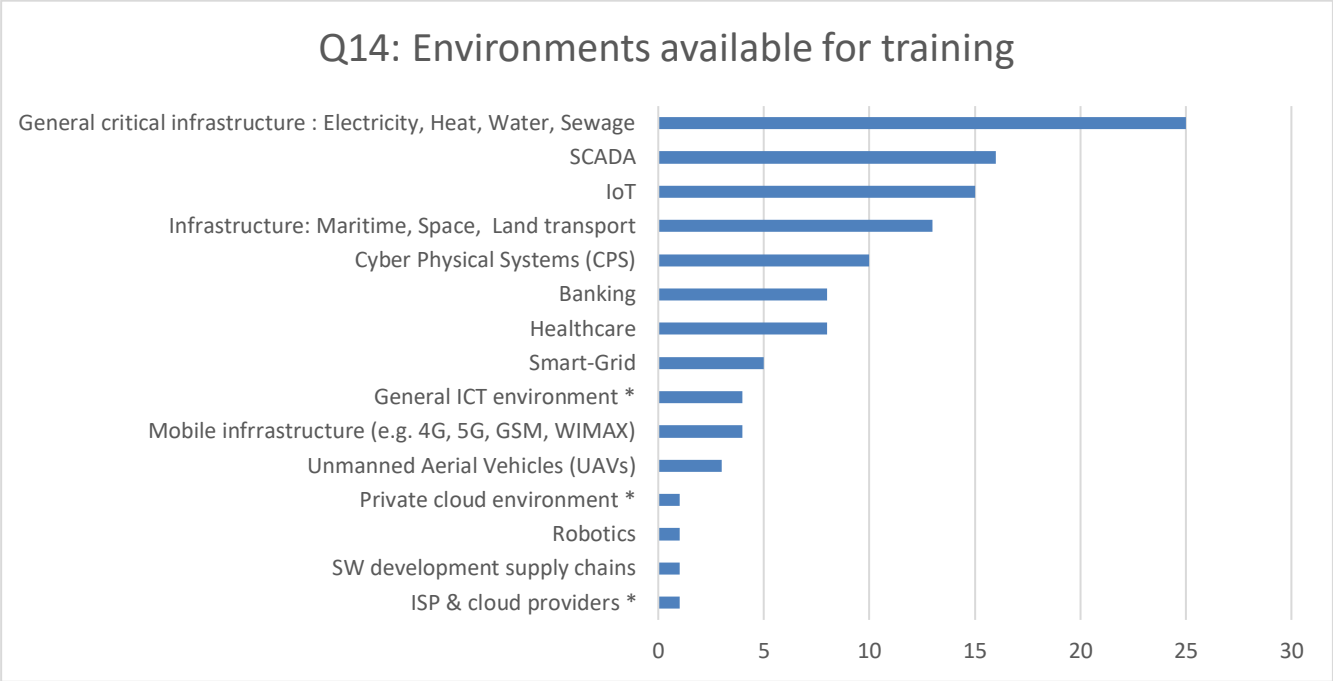

Figure 16: Environments available for training (N=29).

Figure 16 shows the environments available for training. This was a multiple-choice question with 11 options and an "Other" option. 27 of the 29 respondents selected more than one option. There was an open text field to describe other environments available for training and the answers have been included in the figure, marked with an asterisk. The open text field can be considered interesting, as some respondents reported the existence of environments, which the editors had missed whilst planning the survey. The environments listed in descending order are as follows:

- General critical infrastructure: Electricity, Heat, Water, Sewage (25)
- SCADA (16)
- IoT (15)
- Infrastructure: Maritime, Space, Land transport (13)
- Cyber Physical Systems (CPS) (10)
- Healthcare (8)
- Banking (8)
- Smart-Grid (5)
- Mobile infrastructure (e.g. 4G, 5G, GSM, WIMAX) (4)
- General ICT environment * (4)
- Unmanned Aerial Vehicles (UAVs) (3)
- ISP & cloud providers * (1)
- SW development supply chains (1)
- Robotics (1)
- Private cloud environment * (1)

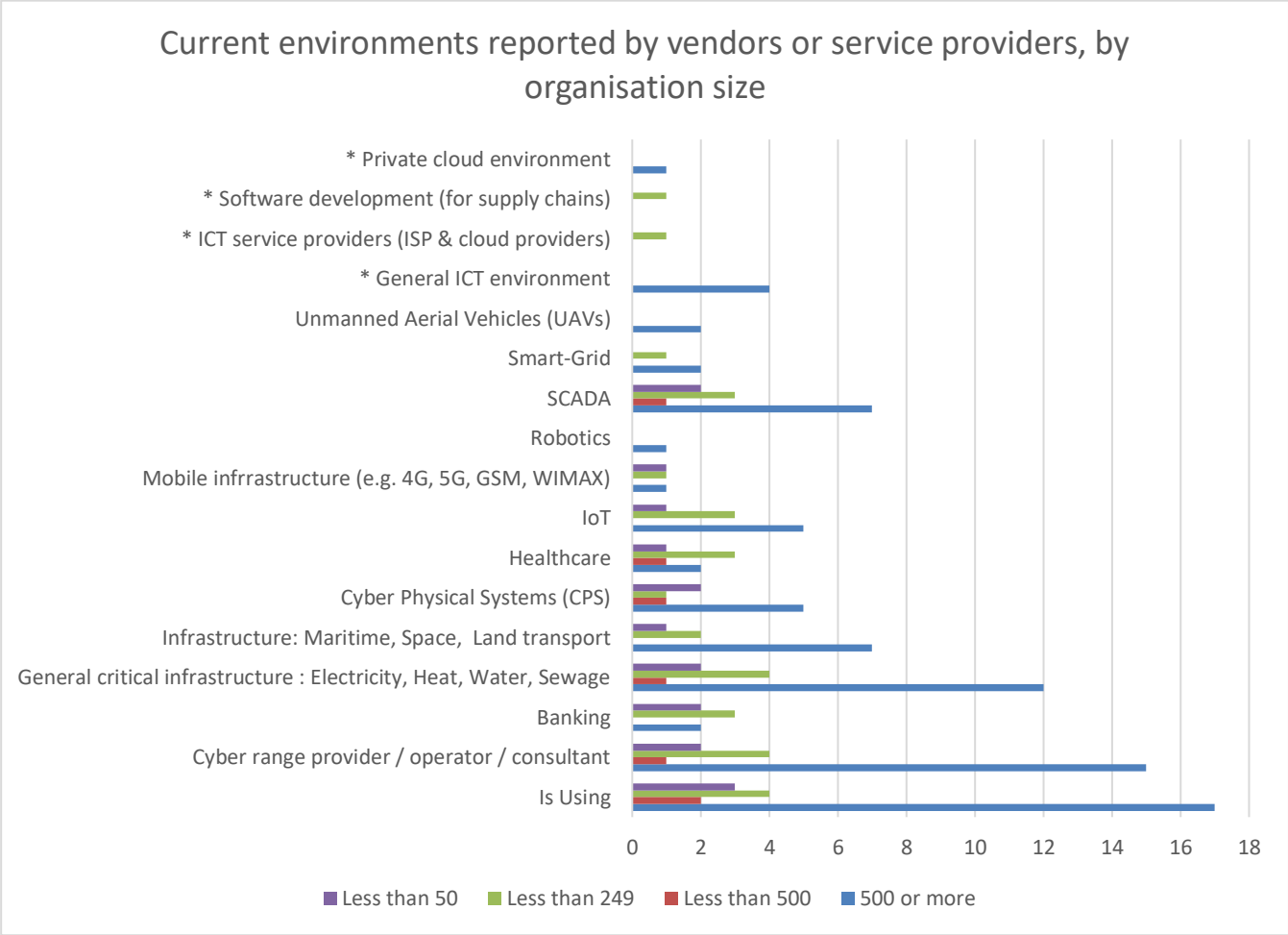

Figure 17: Environments reported by current cyber range vendors or service providers.

Figure 17 shows the currently available environments provided by cyber range vendors or service providers and reported by organisation size. Organisations with 500 or more employees have reported most of the environments – 51, followed by organisations with less than 249 employees, which reported a total of 23 environments. Organisations with less than 50 employees reported a total 12 environments, and organisations with less than 500 employees reported four environments.

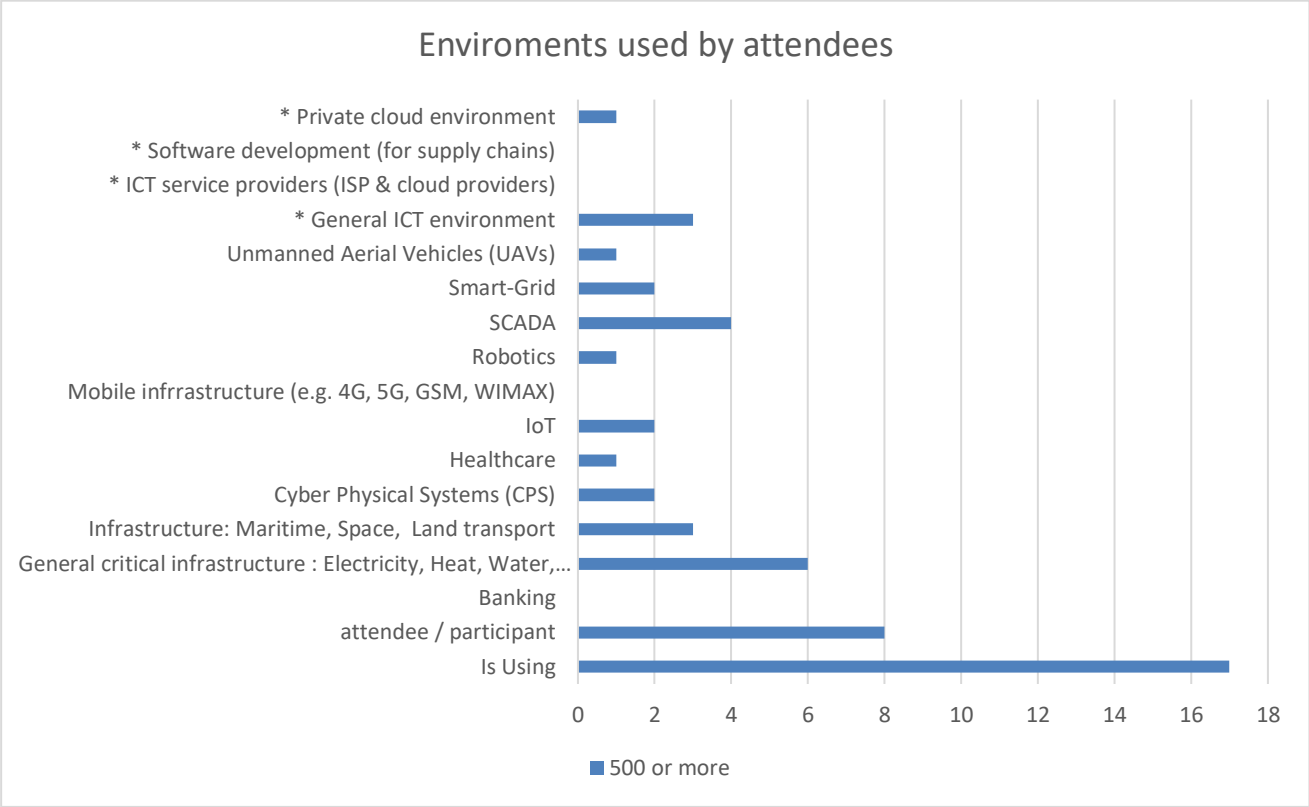

Figure 18: Environments used by attendees (N=10).

Figure 18 shows that only organisations with more than 500 employees reported using a cyber range as attendees or participants and the environments used. It was a multi-choice question, so an organisation may have reported using more than one environment. The environments in descending order are as follows:

- The general critical infrastructure (6)
- SCADA (4)
- General ICT environment (3)
- Smart-Grid (2)
- IoT (2)
- Cyber Physical Systems (CPS) (2)
- Healthcare (1)
- Robotics (1)
- Unmanned Aerial Vehicles (UAVs) (1)
- Private cloud environment (1)
-

Given the small number of answers, no concrete conclusions can be made from the results. Comparing this result to the Eurostat statistics from year 2017 (Eurostat, 2020), which states that most enterprises are SMEs, it may be that the SMEs in EU have no capacity to utilize cyber ranges or they did not respond to the survey. This could be a matter of a future research to clarify.

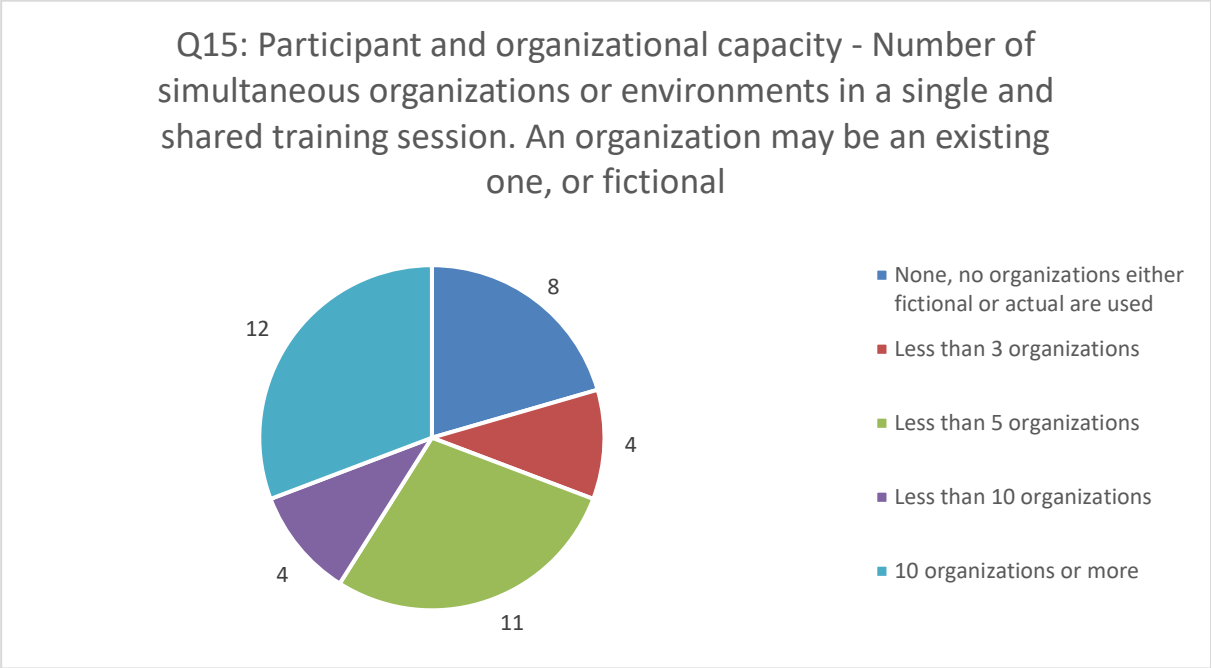

Figure 19: Participant and organizational capacity - Number of simultaneous organizations or environments in a single and shared training session. An organization may be an existing one, or fictional (N=39).

Figure 19 shows the participant and organizational capacity - number of simultaneous organizations or environments in a single and shared training session. An organization in this case may be an existing one, or a fictional organization. 12 (31%) of the respondents answered 10 organizations or more, 11 (28%) less than five organizations, eight (21%) respondents answered none, no organizations either fictional or actual were used, four respondents (10%) less than 10 organizations and four respondents (10%) less than 3 organizations.

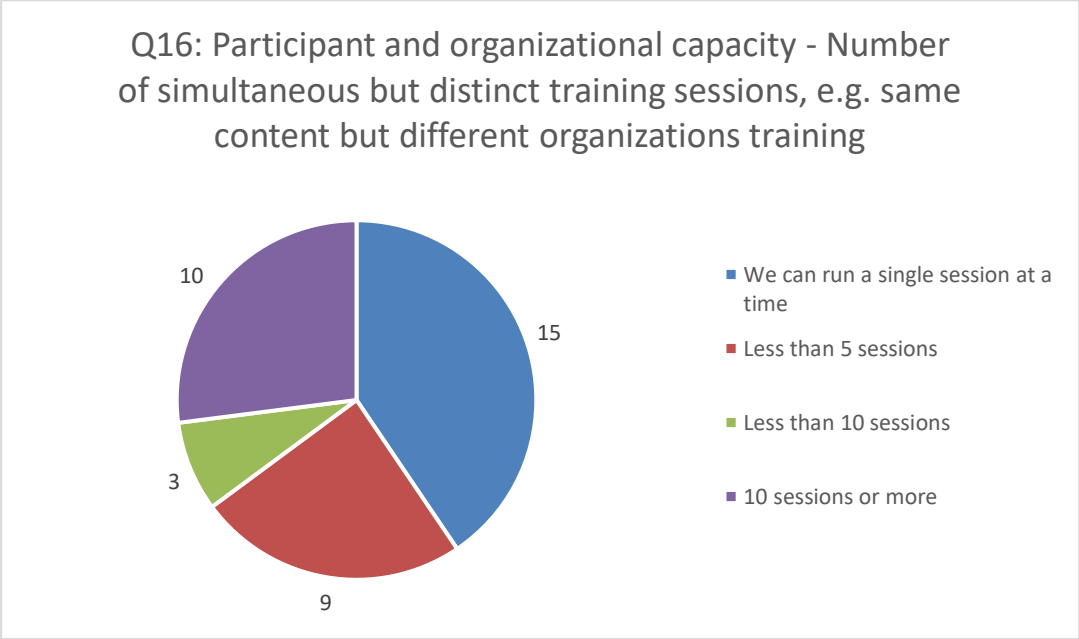

Figure 20: Participant and organizational capacity - Number of simultaneous but distinct training sessions, e.g. same content but different organizations training (N=37).

Figure 20 shows the participant and organizational capacity - number of simultaneous but distinct training sessions, for example same content but different organizations training. 37 of the respondents answered to this question. 15 respondents (41%) answered that they are able to run a single session at a time, 10 responded (27%) that they are able to run 10 sessions or more, 9 responded (24%) that they are able to run less than 5 sessions (meaning 2-4) and 3 responded (8%) that they are able to run less than 10 sessions (meaning 5-9).

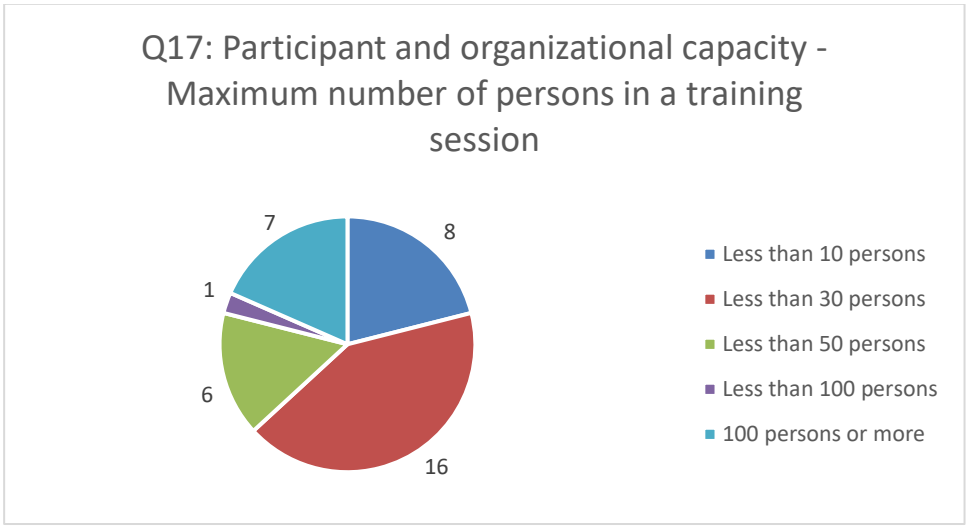

Figure 21: Participant and organizational capacity – Maximum number of persons in a training session (N=38).

Figure 21 shows the participant and organizational capacity - maximum number of persons in a single training session. 16 respondents (42%) answered that the maximum number of persons in a training session is less than 30 persons (meaning 10-29), eight respondents (21%) answered that less than 10 persons (meaning 0-9), seven respondents (18%) answered 100 persons or more, six respondents (16%) less than 50 persons (meaning 30-49) and one answered that less than 100 persons (meaning 50-99).

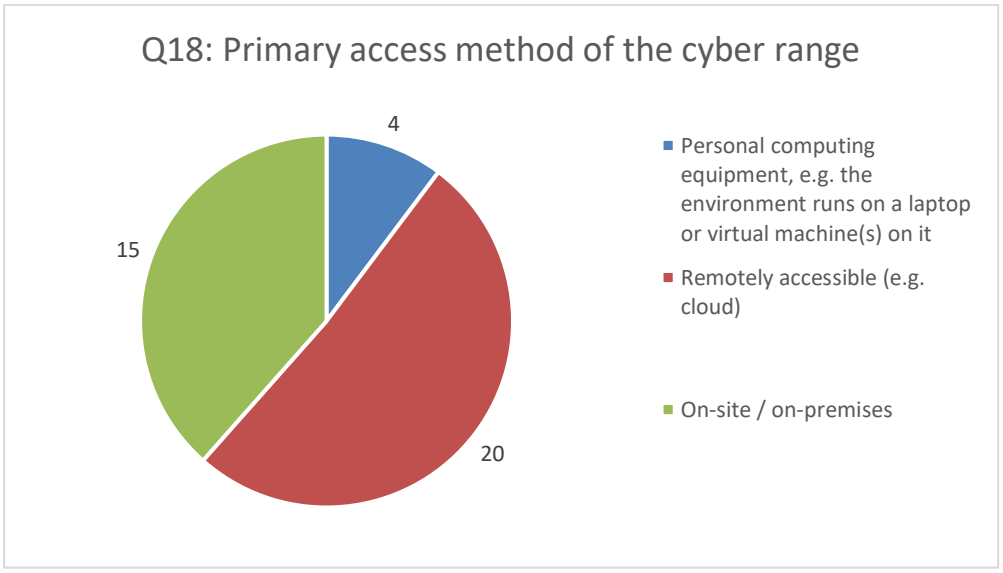

Figure 22: Primary access method of the cyber range (N=39).

The results for the question related to the primary access method of the cyber range are shown in Figure 22. 20 respondents (51%) answered that the cyber range is primarily accessed remotely (for example via cloud), 15 respondents (38%) have access to the cyber range either on-site or on-premises and 4 respondents (10%) have the cyber range environment running on personal computing equipment, for example a laptop or virtual machine(s) on it.

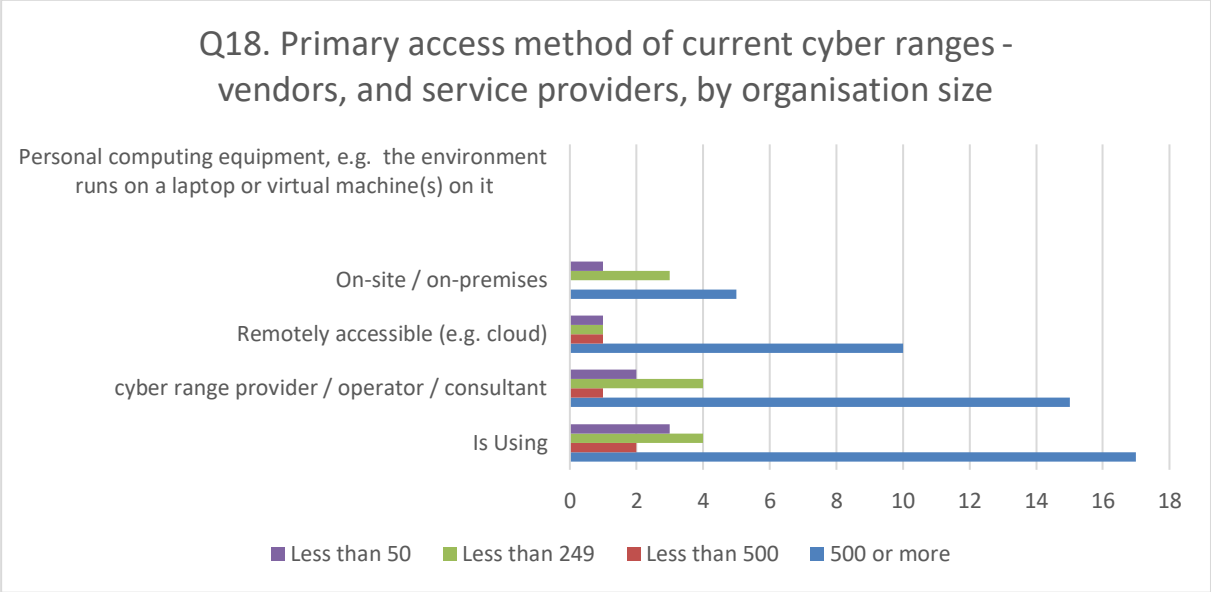

Figure 23: Primary access method of current cyber ranges – vendors and service providers (N=22).

Figure 23 shows cyber range vendors and service providers' statuses regarding the accessibility of current cyber ranges, correlated with organisation size. Most of the environments, 13 (59%) are accessible remotely. Remote accessible were, from organisation size perspective, organisations with 500 or more employees 10 (77%). One respondent from each organisation less than 500, less than 259 and less 50 employees reported having primary access method as remote totalling the rest 23%. On-site access to the environment was reported by total nine organisations (41%), from these five (56%) organisations had 500 or more employees, three (33%) less than 249 employees, and one (11%) less than 50 employees. On-site access were not reported for organisations with less than 249 employees. Organisations with less than 10 employees had not reported being in cyber range vendors or service providers.

Remote accessibility of a cyber range is required to service the exercise and training contents for participants. It also required when interconnecting cyber ranges, by either integrating or performing technical federation. From this perspective there exist potential cyber range partners which could interconnect their cyber ranges in order to offer new or even more realistic contents to participants.

3.3 Performance reporting of cyber range attendees

This category deepens the view of the cyber range in terms of providing information on performance reports and duration of the training session.

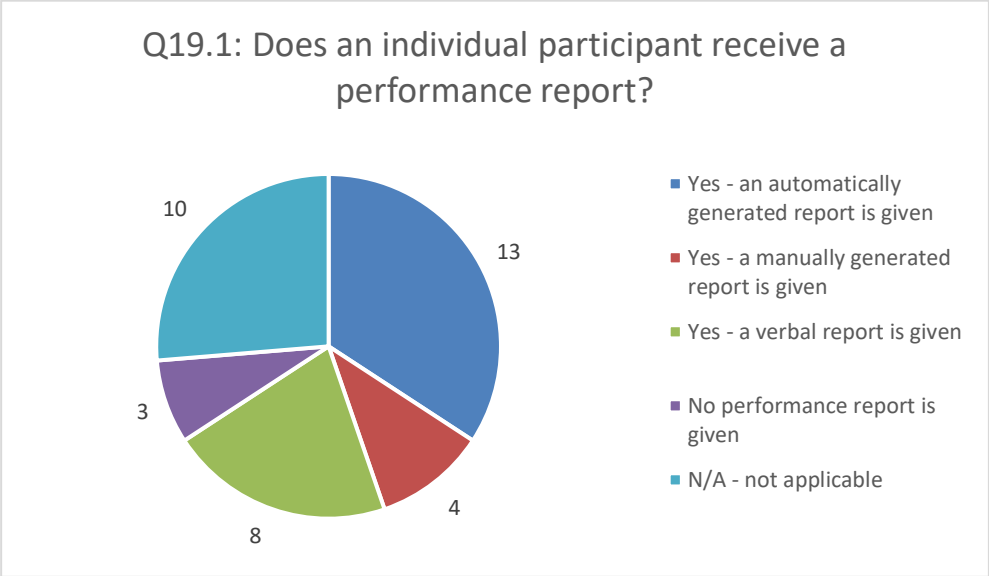

Figure 24: Does an individual participant receive a performance report? (N=38).

Figure 24 answers to question: does an individual participant receive a performance report? 13 respondents (34%) answered that an automatically generated report is given to the participants. Eight respondents (21%) answered that a verbal report is given to the participants, four respondents (11%) answered that a manually generated report is given and three respondents (8%) answered that no performance report is given. 10 respondents (26%) answered N/A – not applicable.

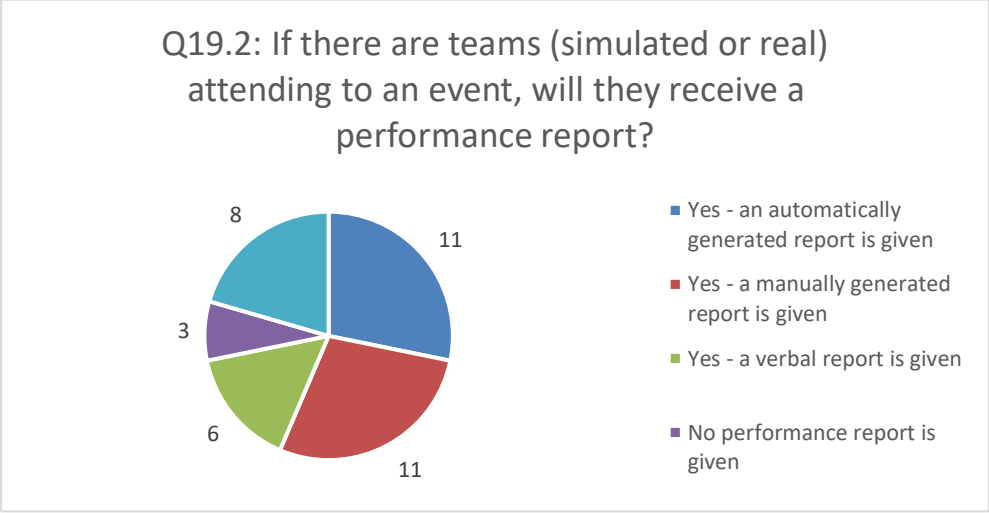

Figure 25: If there are teams (simulated or real) attending to an event, will they receive a performance report? (N=39).

Figure 25 answers to the question: If there are teams (simulated or real) attending to an event, will they receive a performance report? 11 respondents (28%) answered that an automatically generated report is given to the teams and 11 respondents (28%) answered that a manually generated report is given, six respondents (15%) answered that a verbal report is given and three (8%) answered that no performance report is given. Eight respondents (21%) answered N/A – not applicable.

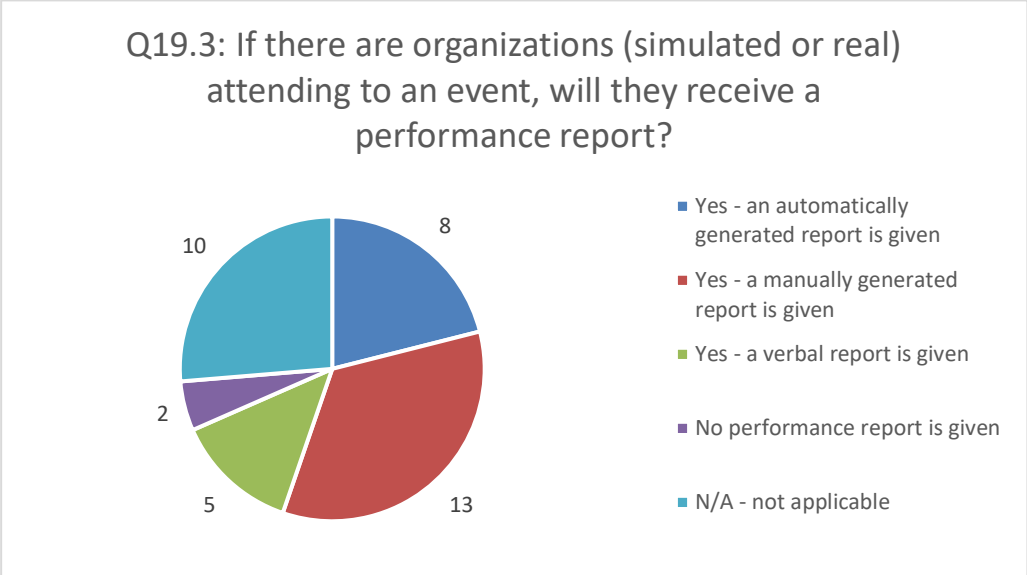

Figure 26: If there are organizations (simulated or real) attending to an event, will they receive a performance report? (N=38).

Figure 26 answers the question: if there are organizations (simulated or real) attending to an event, will they receive a performance report? 13 respondents (34%) answered that a manually generated report is given to the organisations, eight respondents (21%) answered that an automatically generated report is given, five respondents (13%) answered that a verbal report is given and two respondents (5%) answered that no performance report is given. 10 respondents (26%) answered N/A – not applicable.

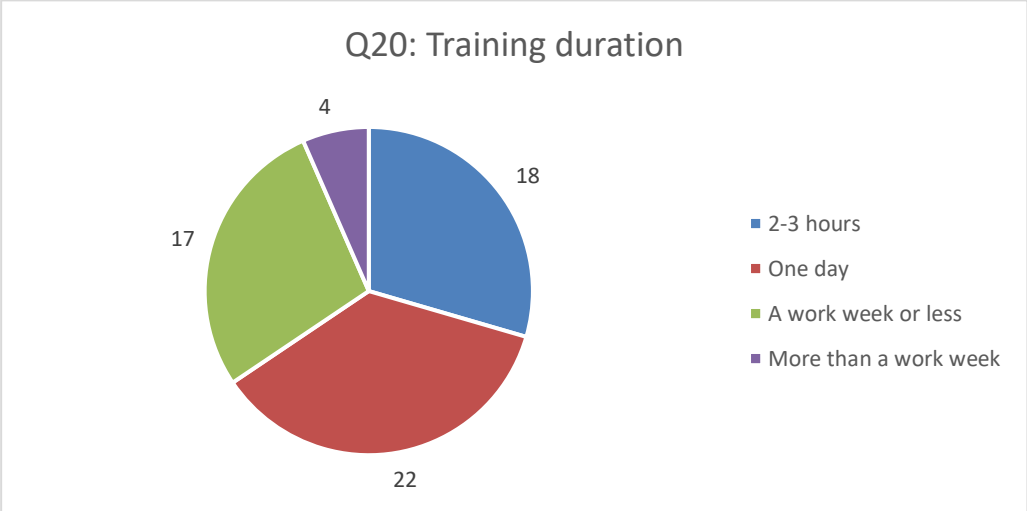

Figure 27: Training duration (N=36).

The training duration, i.e. the upper limit set by the exercise, is shown in Figure 27. There was a possibility to select more than one option in this question and 15 respondents selected more than one option. One day was selected 22 times (36%), 2-3 hours was selected 18 times (30%), a work week or less was selected 17 times (28%) and more than a work week was selected four times (7%).

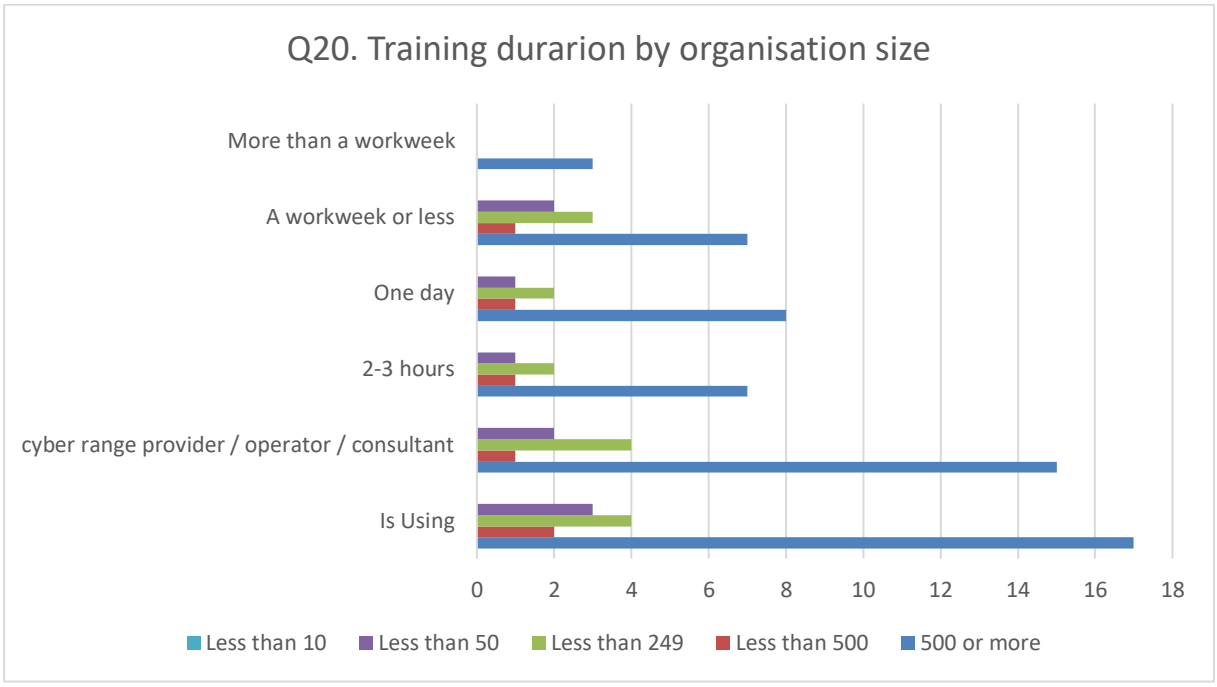

Figure 28: Training duration correlated with organisation size (N=22).

Organisations using and providing cyber ranges or related services reported various durations of trainings held in the environment (Figure 28). The single most selected option was a workweek or less by 13 selections, the One day option was selected by 12 times, and the option 2-3 hours was selected 11 times. Three large organisations selected the option more than a workweek. Organisations having less than 10 persons reported no training durations.

3.4 Cyber Range Technical Specification

This category deepens the view of the technical choices of the specific cyber range. Some of the answers indicate the capability and capacity of the cyber range, some should give indicators of how realistic is the range – compared to real life environments.

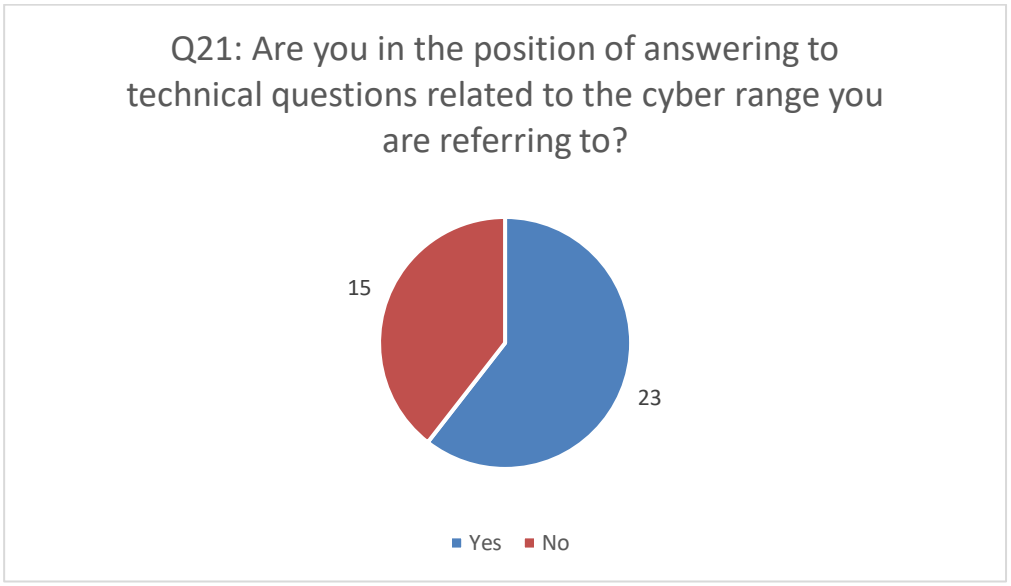

Figure 29: Are you in the position of answering to technical questions related to the cyber range you are referring to? (N=38).

As shown in Figure 29, 23 respondents informed that they are in the position to answer technical questions related to their cyber ranges.

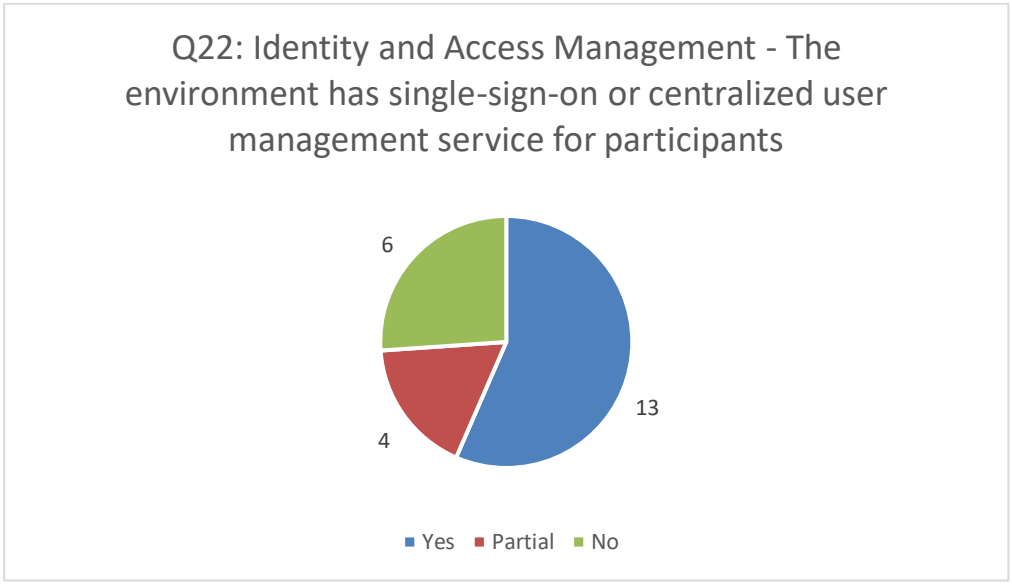

Figure 30: Identity and Access Management - The environment has single-sign-on or centralized user management service for participants (N=23).

Figure 30 shows information on the identity and access management, whether the environment has single-sign-on or centralized user management. 13 (57%) respondents answered that their environment has single-sign-on or centralized user management and six respondents (26%) do not have single-sign-on or centralized user management. Four respondents (17%) answered that the environment has partially single-sign-on or centralized user management.

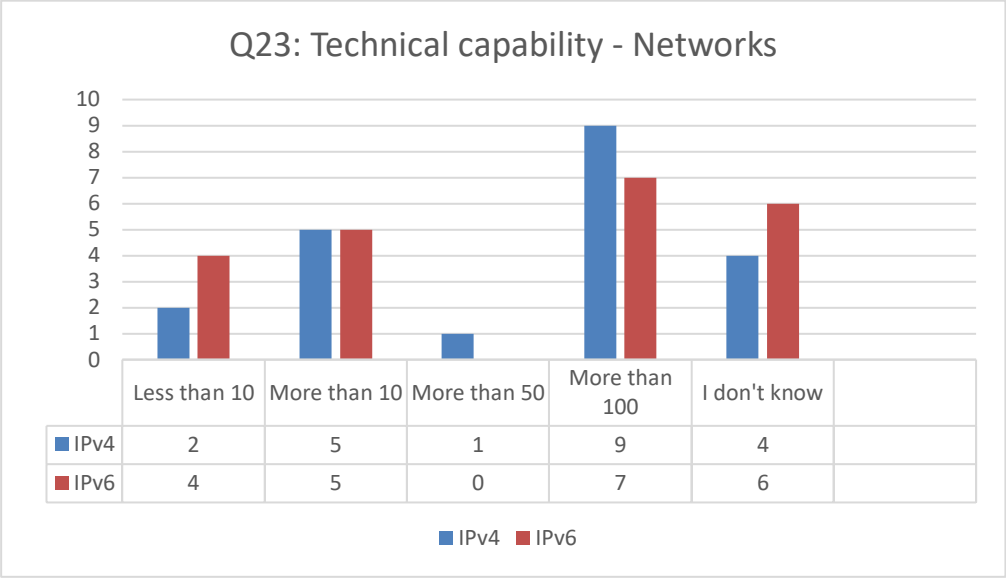

Figure 31: Technical capability – Networks (IPv4 N=21 and IPv6 N=22).

The number of networks: IPv4 and IPv6 is shown in Figure 31. The number of networks indicates how realistic the range might be. Large and realistic environments may have many segmented networks for various purposes, and an Internet facing interface or more instead of the whole organisation running in a single (flat) network and without Internet connectivity. Although there are use cases, where a limited number of networks and no simulated Internet is sufficient to fulfil the requirements of the use case.

Numerical information concerning the number of IPv4 networks was answered by 21 respondents and numerical information concerning IPv6 by 22 respondents. Nine respondents answered that there are more than 100 IPv4 networks in the environment, five answered that more than 10, four that I don't know, two less than 10 and one more than 50. Seven respondents answered that there are more than 100 IPv6 networks in the environment, six answered I don't know, five more than 10 and four less than 10.

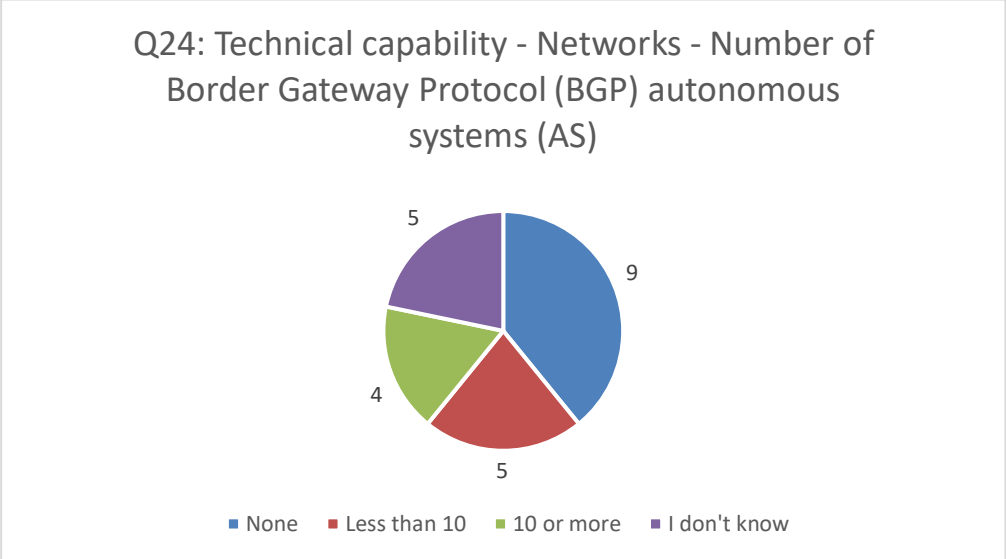

Figure 32: Technical capability - Networks - Number of Border Gateway Protocol (BGP) autonomous systems (AS) (N=23).

The number of border gateway protocol (BGP) autonomous systems (AS) is shown in Figure 32. Nine (39%) of the respondents answered that there are none border gateway protocol (BGP) autonomous systems (AS) in the environment, five (22%) answered that there are less than 10 and four (17%) answered 10 or more. Five respondents (22%) did not know the answer to this question. The number of BGP AS indicates the realism of the simulated Internet in the range.

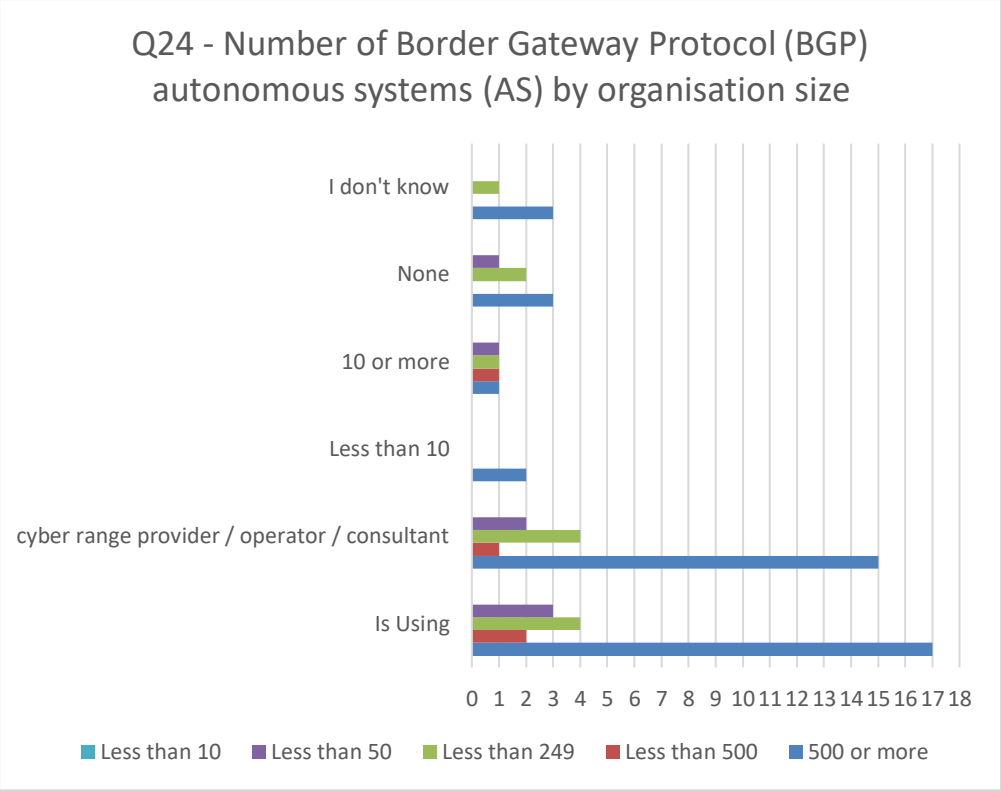

Figure 33: Number of BGP Autonomous Systems correlated with organisation size (N=16).

The currently using organisations currently providing cyber ranges or related services selected BGP AS options as shown in Figure 33. Total six respondents selected an option, stating the cyber range has BGP feature. The option 10 or more ASs was selected once by each organisation size – less than 50, less than 249, less than 500, and 500 or more employees. Two respondents from organisations 500 or more employees selected the option less than 10.

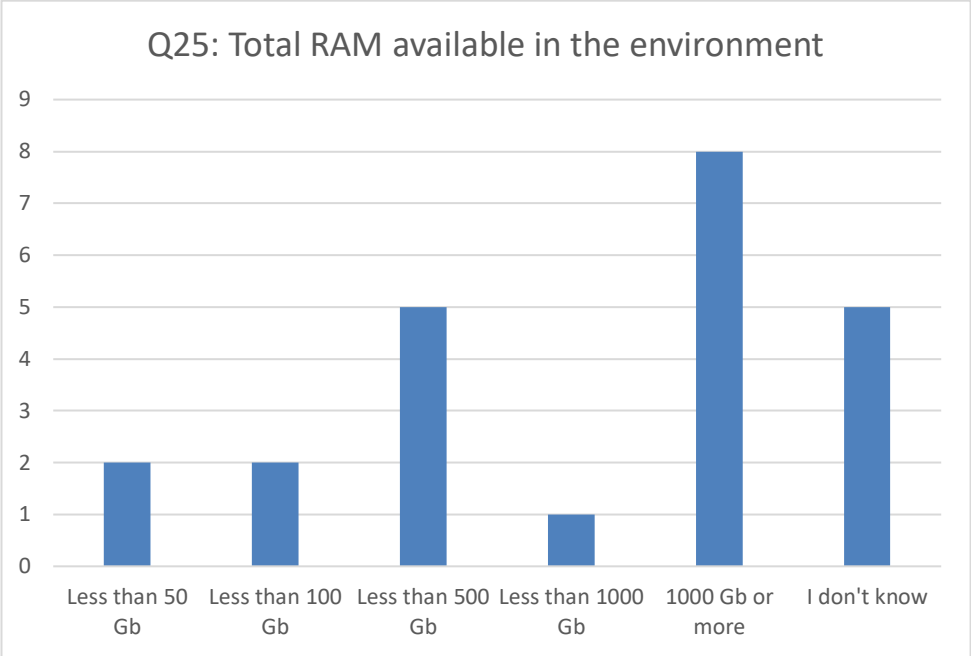

Figure 34: Total RAM available in the environment (N=23).

Figure 34 shows technical capacity concerning computing and specifically total RAM available in the environment. Eight answered that 1000 GB or more RAM is available in the environment, five less than 500 GB (meaning 100-499 GB), two answered less than 100 GB (meaning 50-99 GB) and two less than 50 GB (meaning 1-49 GB). Five respondents didn't know the answer to this question.

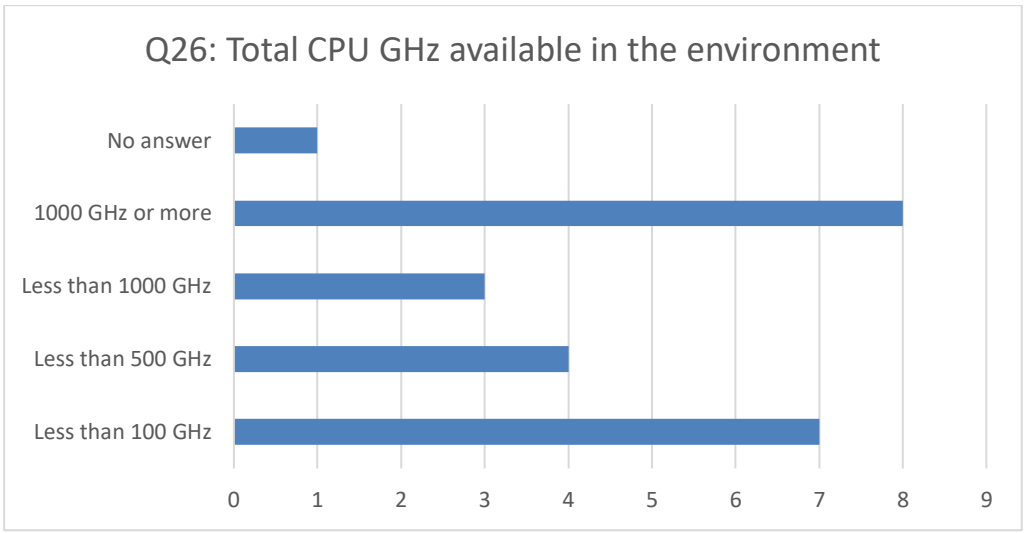

Figure 35: Total CPU GHz available in the environment (N=22).

Figure 35 shows technical capacity concerning computing and specifically total CPU GHz available in the environment. Eight answered that 1000 GHz or more CPU GHz is available in the environment, seven answered less than 100 GHz (meaning 0-99 GHz), four less than 500 GHz (meaning 100-499 GHz) and three less than 1000 GHz (meaning 500-999 GHz). One respondent did not answer this question.

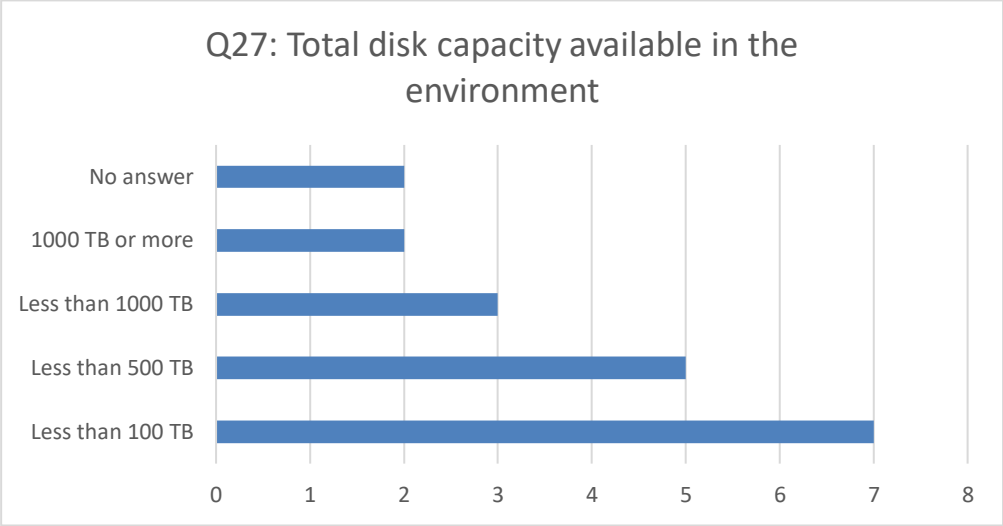

Figure 36: Total disk capacity available in the environment (N=21).

Figure 36 shows technical capacity concerning computing and specifically total disk capacity available in the environment. Seven answered that less than 100 TB (meaning 0-99 TB) is the total disk capacity available in the environment, five answered less than 500 TB (100-499 TB), three answered less than 1000 TB (meaning 500-999 TB) and two 1000 TB or more. Two respondents did not answer this question.

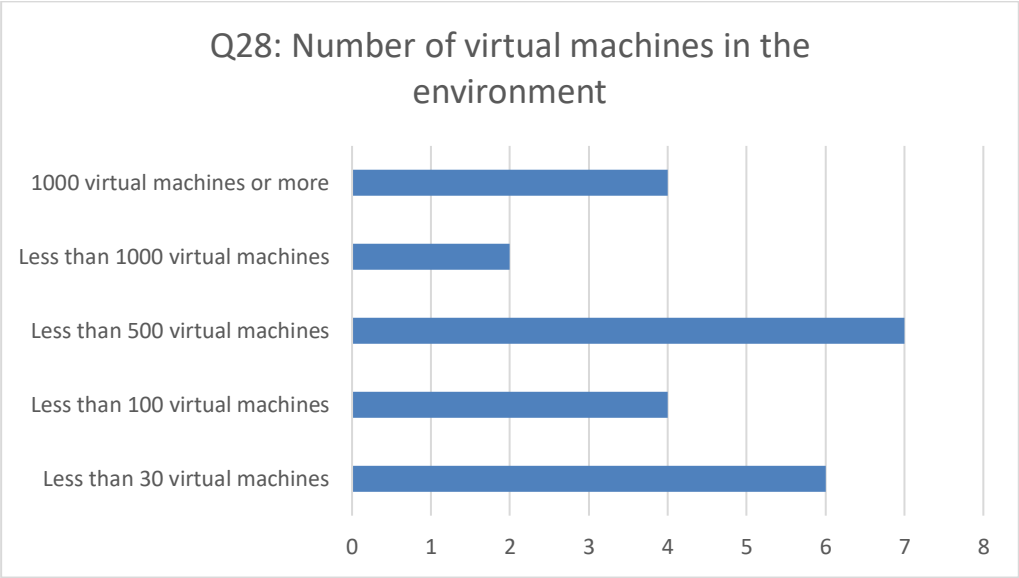

Figure 37: Number of virtual machines in the environment (N=23).

Figure 37 shows technical capacity concerning computing and specifically the number of virtual machines in the environment. Seven answered that there are less than 500 virtual machines (meaning 100-499 virtual machines) in the environment, six answered less than 30 virtual machines (meaning 0-29 virtual machines), four answered 1000 virtual machines or more, four less than 100 virtual machines (meaning 30-99 virtual machines) and two less than 1000 virtual machines (meaning 500-999 virtual machines).

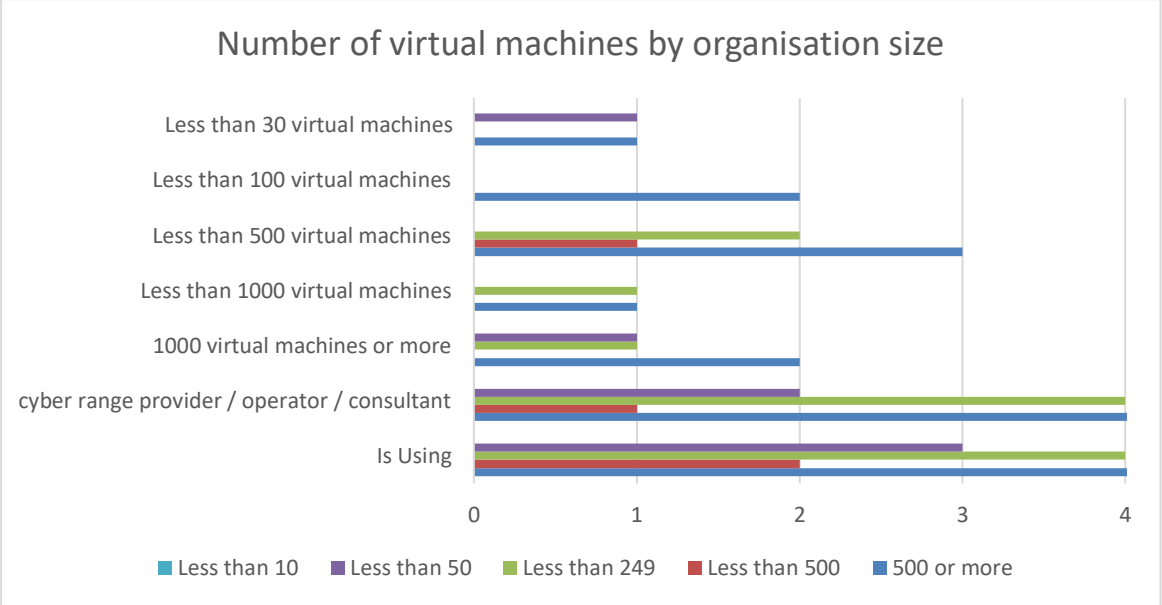

Figure 38: Number of virtual machines by organisation size, current cyber range vendors or service providers (N=22).

Number of virtual machines by organisation size is shown in Figure 38. Less than 30 virtual machines were selected by two respondents (9%), one organisation with less than 50 and one with 500 or more employees. Less than 100 virtual machines were selected by two respondents (9%) from organisations with 500 or more employees, less than 500 virtual machines were selected by six (27%) respondents, three from organisations with 500 or more employees, two organisations with less than 249 employees and one organisation with less 500 employees. Less than 1000 virtual machines were selected two (9%) times, one organisation more than 500 and one organisation less than 249 employees. 1000 or more virtual machines were selected four times (18%), two organisation with 500 or more, one organisation less than 249, and one by organisation less than 50 employees. Not all respondents answered to the question.

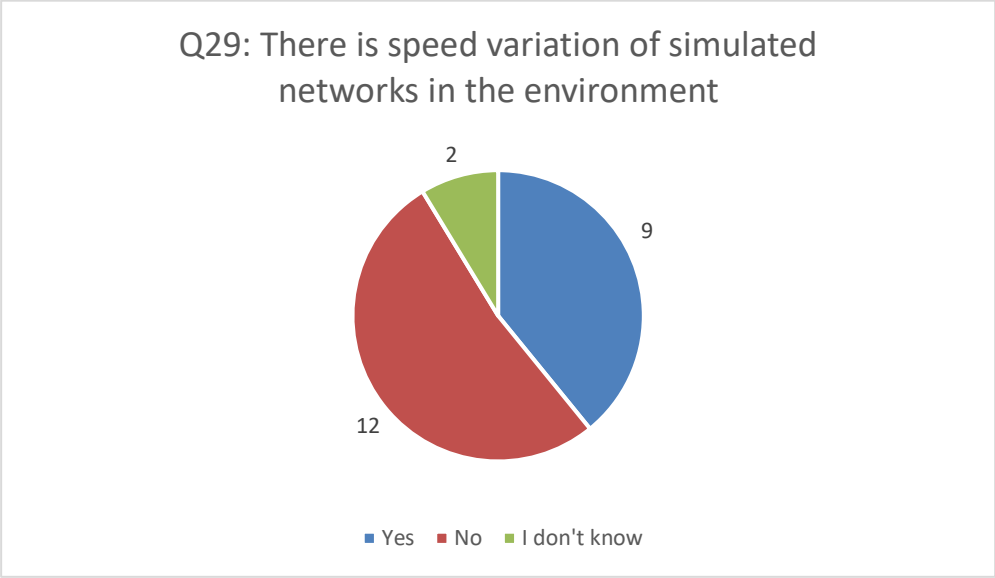

Figure 39: There is speed variation of simulated networks in the environment (N=23).

Speed variation occurs in the Internet between ISPs thus affecting the end user(s), in office and home networks, and may occur even in operational networks. Figure 39 gives an answer to the question: is there speed variation of simulated networks in the environment? 12 (52%) respondents answered there is no speed variation of simulated networks in the environment, nine (39%) answered yes. Two respondents (9%) didn't know the answer to this question.

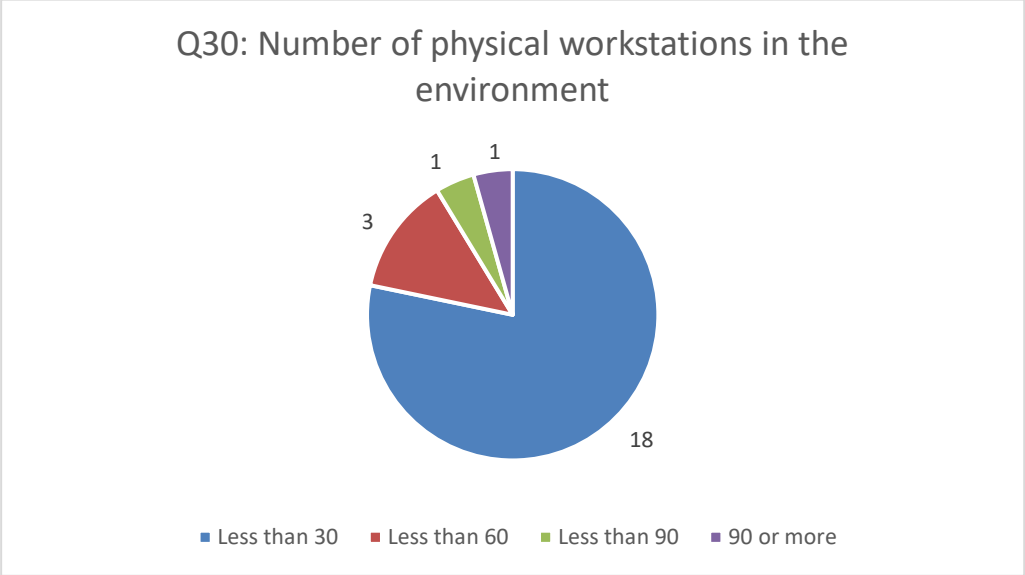

Figure 40: Number of physical workstations in the environment (N=23).

Number of physical workstations in the environment is shown in Figure 40. 18 respondents (78%) answered that there is less than 30 (meaning 0-29) workstations in the environment, three (13%) answered less than 60 (meaning 30-59 workstations), one (4%) answered less than 90 (meaning 60-89 workstations) and one 90 or more workstations.

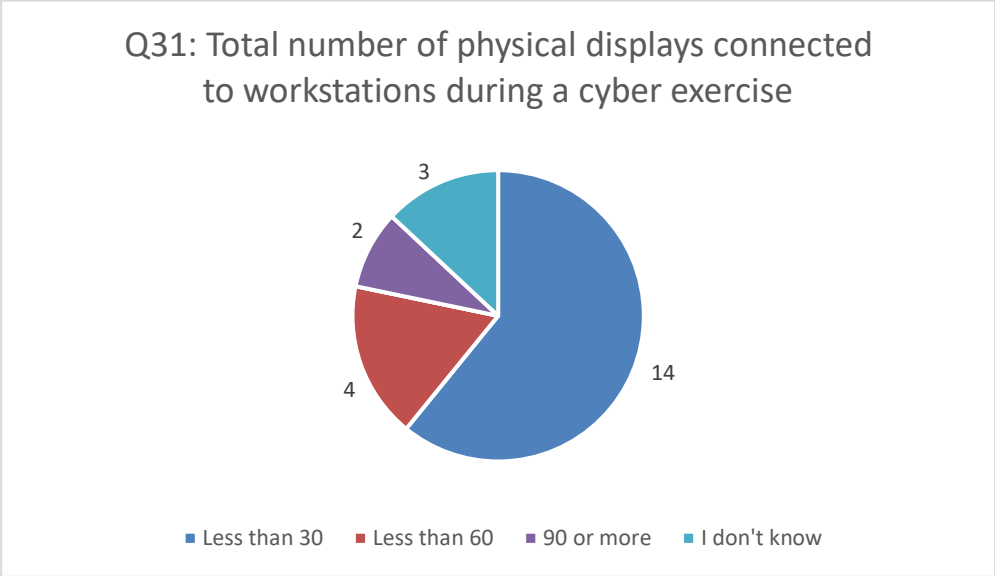

Figure 41: Total number of physical displays connected to workstations during a cyber exercise (N=23).

Figure 41 shows the total number of physical displays connected to workstations during a cyber exercise. 14 respondents (61%) answered less than 30 (meaning 0-29) physical displays are connected to workstations during a cyber exercise, four (17%) answered less than 60 (meaning 30-59 displays) and two (9%) answered 90 or more. Three respondents (13%) did not know the answer to this question.

3.5 Cyber Range Federation

This category gives views on the implementation and plans for implementing interconnection of the cyber range with one or more other environment(s) and the cross-use of each other´s services via this technical federation in a joint event or exercise.

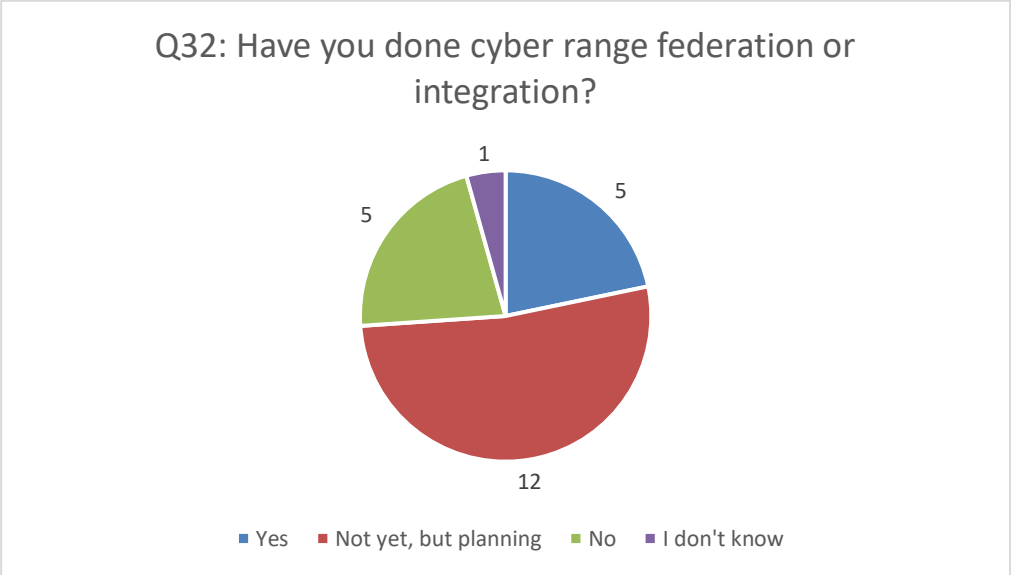

Figure 42: Have you done cyber range federation or integration? (N=23).

Figure 42 shows whether the respondent has interconnected or has plans to interconnect the cyber range with one or more other environment(s) and to cross-use each other´s services in a joint event or exercise. 12 respondents (52%) answered that they have not yet done federation or integration but have plans to do, five respondents (22%) answered no and five respondents (22%) answered yes. One respondent didn't know the answer to this question.

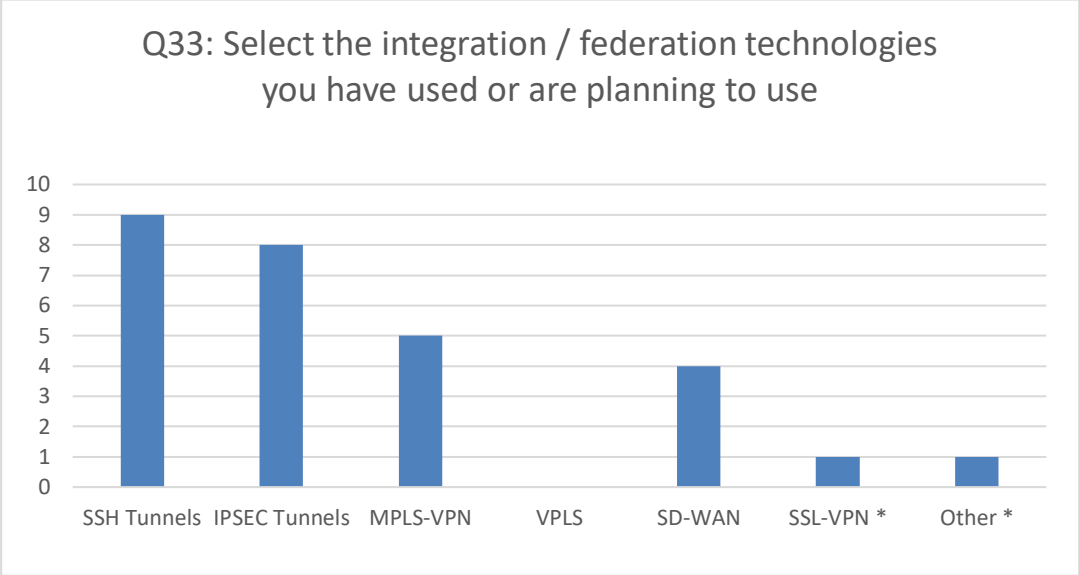

Figure 43: Select the integration / federation technologies you have used or are planning to use (N=16).

For those who answered that they have done or have plans to do federation or integration a question concerning the integration / federation technologies used or planned to use was presented and the answers are shown in Figure 43. 16 respondents answered this question. There was a possibility to select many options and seven (56%) respondents selected more than one option. SSH tunnels was selected nine times, IPSEC tunnels eight times, MPLS-VPN five times and SD-WAN four times. There was an open text field to describe other technologies and the two answers have been included in the figure, marked with an asterisk.

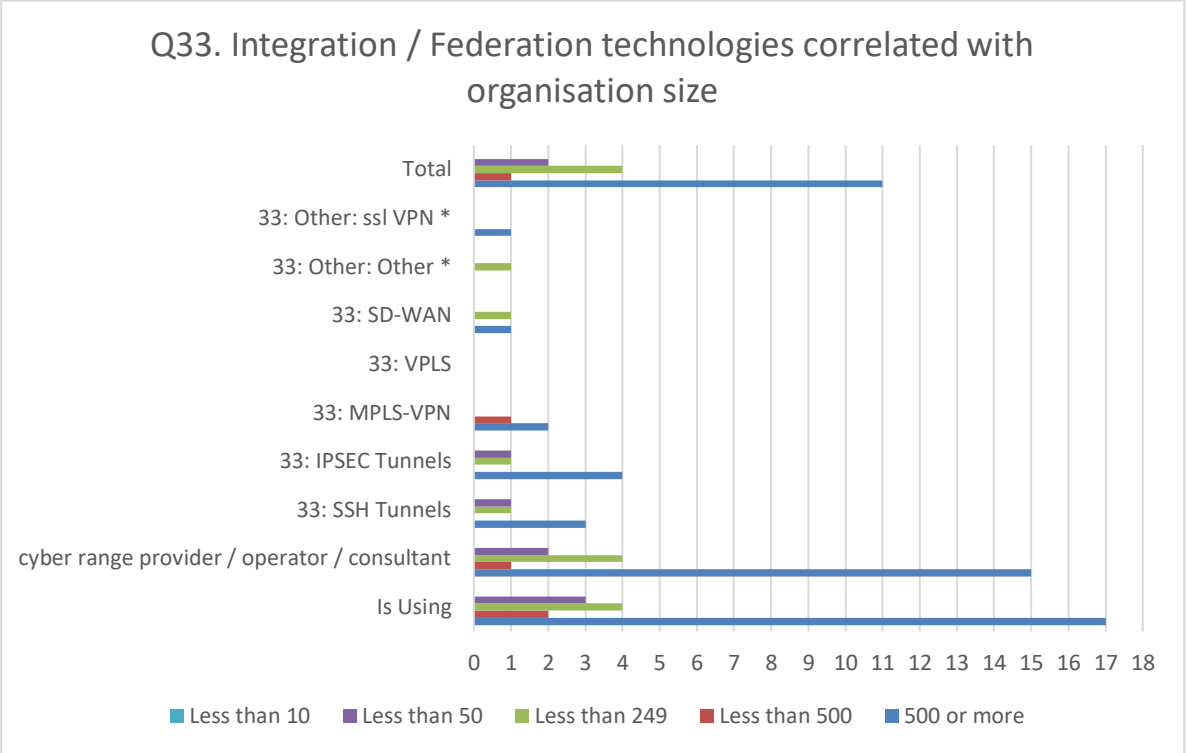

Figure 44: Integration / Federation technologies correlated with organisation size.

Used integration or federation technologies correlated with organisations size, for organisations currently using or providing cyber ranges or related services, is shown in Figure 44.

Organisations with 500 or more employees selected IPSEC tunnels four times, SSH tunnels three, MPLS-VPN two, both SD-WAN and SSL-VPN, which was entered in an open text field, received one selection from organisations with 500 or more employees. Organisations with less than 500 employees had selected only MPLS-VPN option. Organisations less than 249 employees had reported one selection for each IPSEC tunnels, SSH tunnels, SD-WAN and for unspecified open text other. Organisations with less than 50 employees selected one time IPSEC tunnels and SSH tunnels. Organisations with less than 10 employees did not report any integration or federation technologies. No selections were made to option VPLS.

3.6 Cyber Range Connectivity

This category gives further information on the cyber range´s Internet connectivity, whether it is dedicated or not, details on the connectivity speed and latency (Round-Trip-Time).

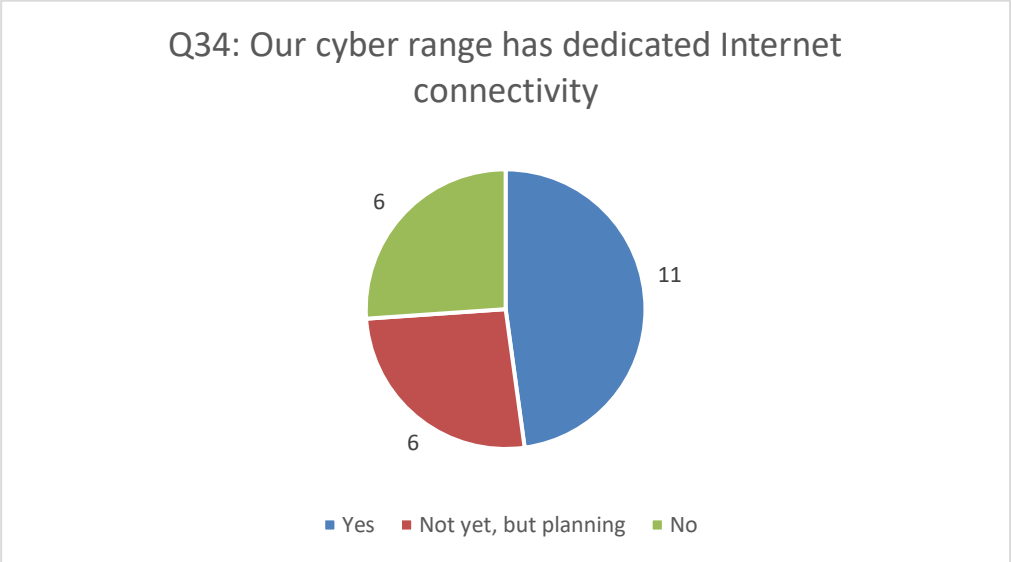

Figure 45: Our cyber range has dedicated Internet connectivity (N=23).

Dedicated Internet connectivity for a cyber range enables trainings and exercises in the environment that do not interfere with organisations other activities and vice versa. Figure 45 shows answers to question: does the cyber range have a dedicated Internet connectivity? 11 respondents (48%) answered that the cyber range has dedicated Internet connectivity, six (26%) answered not yet, but planning to have and six (26%) answered no.

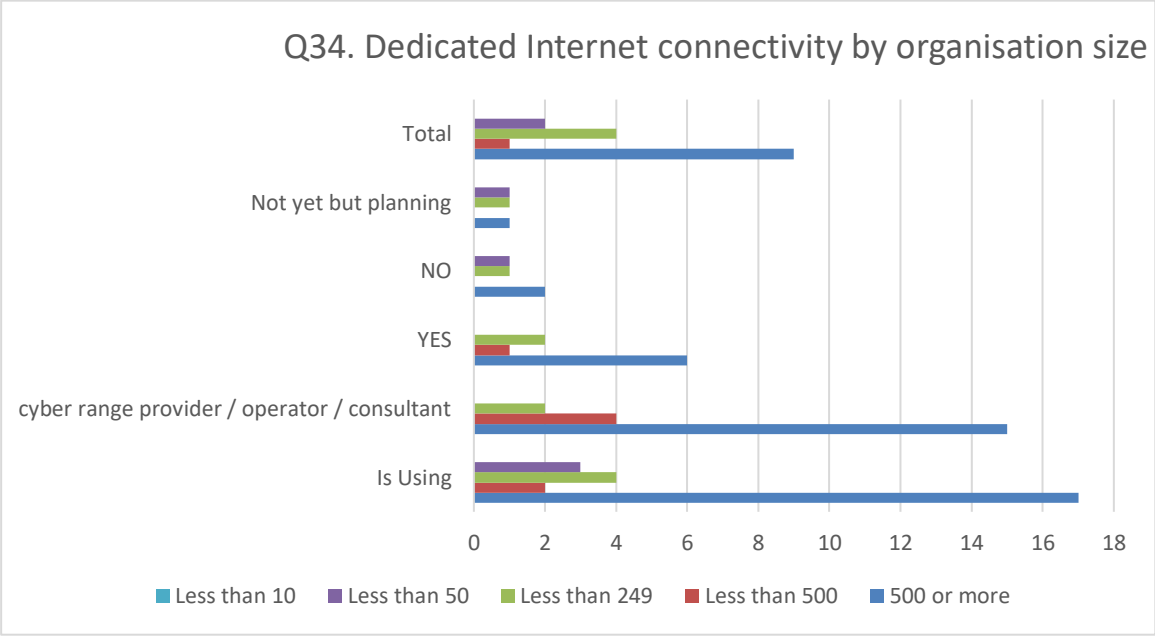

Figure 46: Dedication Internet connectivity correlated with organisation size.

Figure 46 shows that organisations currently using or providing cyber ranges or related services, total nine selections was made for the option Yes, four selections was made for No option, and the option Not yet, but planning was selected three times. For organisations with 500 or more employees, most selected option was Yes with six selection, option No was selected two times and one selection was made for Not yet but planning. For organisations less than 500 employees, one selection was made for

option Yes. Organisations with less than 249 employees option Yes was selected by two respondents, option No and Not yet but planning were both selected by one respondent. Organisations with less than 50 employees reported one selection for No and Not yet but planning. Organisations with less than 10 employees did not report any option.

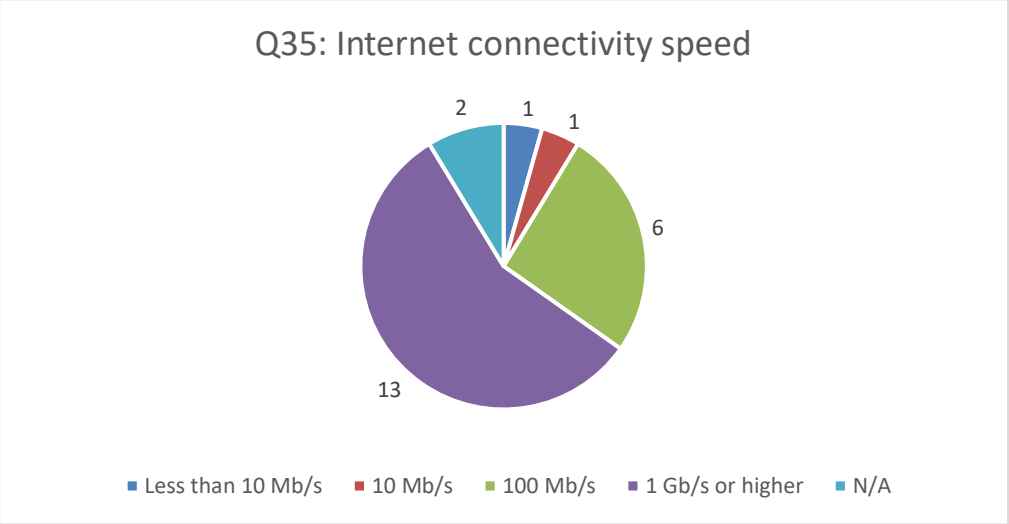

Figure 47: Internet connectivity speed (N=21).

Figure 47 shows integration or federation capabilities in terms of Internet connectivity speed. 13 respondents (57%) answered that the Internet connectivity speed is 1Gb/s or higher, six (26%) answered 100 Mb/s, one answered less than 10 Mb/s and one answered 10 Mb/s. Two respondents did not answer this question.

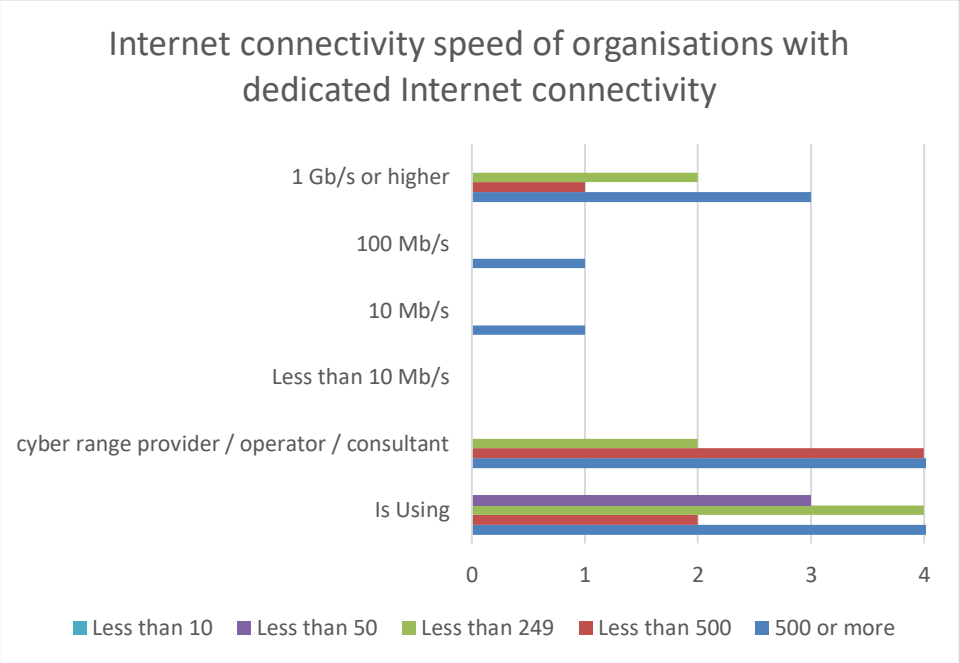

Figure 48: Internet connectivity speed of organisations with dedicated Internet connectivity.

Figure 48 shows reported connectivity speed of organisations with dedicated Internet connectivity, correlated with organisation size. Single most selected option was 1 Gb/s or higher with total six selections. It was selected by organisations with less than 249 employees (2), organisation with less than 500 employees (1) and organisations with 500 or more employees (3), which also selected once the options 100 Mb/s and 10 Mb/s.

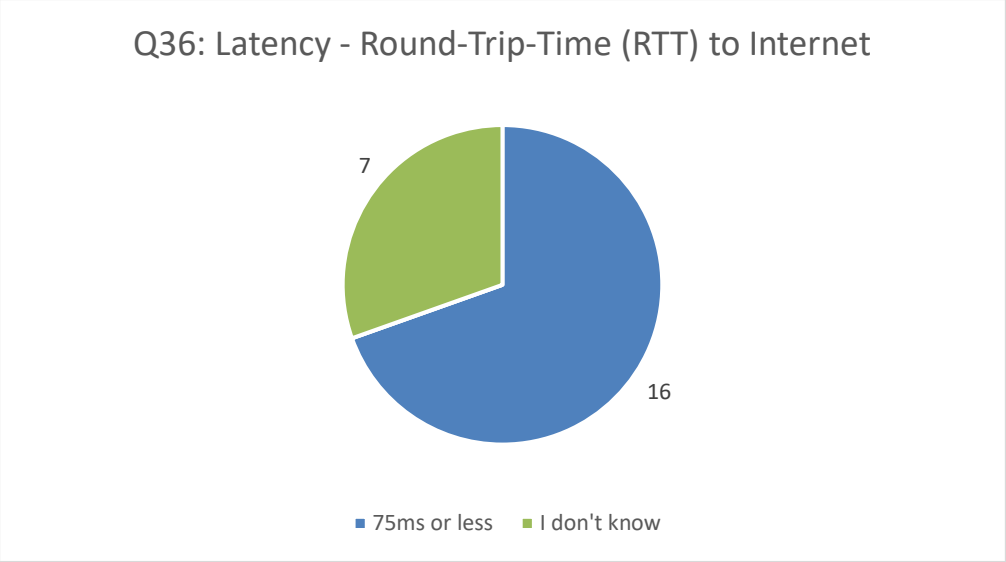

Figure 49: Latency – Round-Trip-Time (RTT) to Internet (N=23).

Figure 49 shows the latency - Round-Trip-Time (RTT) from the organization to the Internet Service Provider. The respondents were advised to execute the command "ping 8.8.8.8" and report the average round trip time if the question was hard to answer. 16 (70%) answered that the RTT is 75ms or less and seven (30%) answered I don't know. None of the respondents selected the over 75ms RTT option.

4 Interview Results

Qualitative interviews were performed for survey respondents who had given their approval to be reached and had indicated that they have done federation. Four respondents matched these criteria and were contacted for further interviews. An interview with three of these four respondents was organized, since one respondent could not schedule the interview. The interview questions (Annex B: Interview questions) made in advance were provided to the respondents before the interview for them to be able to prepare themselves. The interviews had a strict time limit of 20 minutes. This time was selected based on the assumption that the interview candidates could fit the interview into their calendars with short notice. The interview had mandatory questions (1-7), and questions that were asked if the time limit allowed (8-11). Each remotely held interview session was formed by two CyberSec4Europe members and the interviewee. Interviews were recorded and transcribed. Interviewees are presented pseudonymously.

The cyber ranges interviewees had different backgrounds. The first interviewee said the company had done several installations using a commercial cyber range in few European countries. The second interviewee said that its organisation has in-house specified, developed and operated large-scale live cyber ranges. The third interviewee said that the company the person works for has an in-house developed cyber range, but primarily the person referred to a publicly funded project's cyber range which is currently being developed.

All the respondents described the environment they each referred to as a cyber range. All of the interviewees were familiar with ECSO report "Understanding cyber ranges: from hype to reality". The verbal description of a cyber range could be summarised as this definition of cyber range is fulfilled only if the features, functionalities, capabilities and resources of the range enables running cyber exercises, trainings, research and development, testing and potentially certification. In the survey, all the interviewees had answered that they are cyber range (service) providers, operators or consultants.

When asked about any requirement specification document or reference of such a cyber range federation, the interviewees stated there were no requirements for federation, or they were for internal use or for restricted audience.

For further details, the interview transcription is provided in chapters below.

4.1 Benefits of Cyber Ranges

When asked about the benefits the interviewees were expecting or gained of cyber range federation, the answers varied as seen below.

First interviewee

> *We opened up the first lab in one country, after that expanded to three other countries. We built the federation in a sense that we created the community of people working in different ranges, we were exchanging resources, sharing scenarios, virtual machines (by depository) and expenses. We did not manage at that point to technically interface the environments, I mean physically connect, we were about to do it, but we realized that the main use cases or the main benefits for federation was exchange of knowledge and expertise rather than broaden the cyber range virtual network itself. Beneficial was exchanging scenarios and test capabilities we had.*

Second interviewee

> *Technical perspective of the federation, most of the benefits are that you can integrate different environments for more comprehensive set of functionalities and options to use in exercises or trainings or other kind of activities you utilize the cyber range for. Basically that is the idea behind the federation, so you can bring more functionalities for different kinds of cyber ranges that others do not necessarily have, so that is the main idea of federation and the other side is that you can scale up if the cyber ranges are small and are part of the federations we can integrate/ interconnect those together so we can scale up the resources for larger scale exercises and larger scale trainings as well*
>
> Question: Is federation permanent or use case based?
>
> *Depends on the cyber range usage, from our perspective always case by case since we already have a large scale cyber range and are not lacking that many features that we want, so it is based on certain cases that we need a federation for with somebody else, it can be for example a multinational exercise that demands that the multinational partners connect from the national range to each other. One multinational case example could be that all national participants connect to the national level cyber ranges and the cyber ranges are federated/ interconnected to each.*

Third interviewee

> *There are mainly two benefits (one is more technical and one commercial)*
>
> *- one is a possibility to create more complex scenarios (when federating more than one range) this is valuable from multisector simulation perspective*
>
> *- Another benefit is the concept of marketplace, so the possibility to have a single marketplace where multiple cyber range providers/ content (scenario) providers can publish their services,*

Amazon like environment, since the market is very scattered, clients claim it is hard to find cyber range services (they don't know exactly what they need, where to ask, from who to ask and they normally start with the big players and the big players can't maybe provide what they need and it is very difficult).

4.2 Cyber Range Federation – is it Operational or Technical?

Interview questions three and four were formulated in a way that the interviewee should elaborate on the possible differentiation of the definition of cyber range federation, is it operational or technical, or something else from their perspective. Question three was "*By stating that you have done federation or are planning to do it, a question about the federation term. Do you find that Federation is sharing scenarios or other operative data related to an exercise in machine readable form being Operational Federation?"*

First interviewee

Yes (this gave most benefit), I would also highlight that when we were changing experiences we were also exchanging VMs and libraries of content, it was important for us to be able to exchange easily the machines and luckily we had the same suppliers so it allowed easy exchange of VMs. That was a key element, in the federation, in the sense we see it and that is why we did not need to interconnect the labs since we were able to just exchange the images of the virtual machines from one range to another via a depository somewhere, that was enough.

Second interviewee

We have been using many times the technical federation term when we have been talking about federation to make it sure everybody understands the term, that it is about interconnecting the cyber ranges and bringing the features of the cyber ranges together and being able to use multiple features around the different cyber ranges in a common or joint exercise.

I agree we need a more specific taxonomy & terminology for federation, I wouldn't say right away that federation is about sharing scenarios and operative data, in my opinion it can be just technical stuff (sharing the features, sharing the resources) in one perspective but on the other hand it also can be joined scenarios, shared scenarios, but depending on the environments and the structures and topologies and capabilities of the cyber ranges the sharing of the scenarios is not that simple right away so, depending on where the scenario has been created in, it is not that easily utilized by somebody else that does not have the same kind of environment or same kind of topologies or capabilities inside of the cyber range.

So, it is a tricky situation in my opinion at the moment. I want to add here that it will be more difficult because of the nature of the cyber ranges that are so different from each other.

Third interviewee

A note from the editors: the person works for a company which has cyber range technology and related services (The company), and the person works for a publicly funded project (The project) developing cyber range federation technology and related services. The editors have added their viewpoints to the text.

[The project] view is that when a customer wants a customised scenario, what we are developing is a scenario description language that collects customer requirements in a machine and human readable language that is converted to a capacity capability data model, which is shared among the cyber range providers, which could provide these custom scenarios.

[The project] goal is to find common shared language, to customers/ providers to share when they are defining and talking about cyber ranges services

Federation needs to be absolutely agile; the system needs to work in all cases

The fourth question was "*By stating that you have done federation or are planning to do it, a question about the federation term. Do you find that Federation is technically (at network level) sharing network resources or services therein, being Technical Federation?"*

First interviewee

We created links through VPN (hybrid connection) the ability to connect to the outside world and each of the ranges were connected to an Internet gateway and basically we created a VPN connection between two gateways, but we never used an exercise or training which required multi-site, connection

Interfacing / interconnecting ranges were the terms used internally when speaking of federation (although federation term was understood by all as well).

Second interviewee

I agree the technical federation is about sharing the resources and services inside of the cyber ranges, so not just the computing power, but especially about the cyber range services for the exercises, it can be exercise management it can be blue team environments it can be global Internet environments it can be other kind of testbed environments that are brought to be part of the larger scale exercises and so on. Technical federation in my opinion is clearer because we talk about the technical interconnection and sharing of the services.

Third interviewee

[The project] calls it interconnection, because federation is more complex than technical interconnection, for complete federation a technical federation is of course needed.

4.3 Certification Requirements in Cyber Range Context

Related to certification, the interviewees were asked whether they had requirements for the environment they referred, for the facilities in which the environment is operated, or the staff operating or accessing the environment. Also it was asked, if the interviewee could share the standard they might be referring to.

First interviewee

Not from our side, the engineers working had certifications, but it was not obligatory. The question is interesting, I think it would be valuable to define a joint or recognized certification for cyber ranges since even today the term cyber ranges can be understood differently and it could

help to have this common understanding, taxonomy and language when we speak of cyber ranges.

Second interviewee

There is no common shared certification currently for the cyber ranges or facilities used at the moment, some of the customers may be requiring certain certification, certain things, classified facilities etc., but those are always done together with the customer, so it is not a common framework in a sense.

When asking for a reference of a standard: "*In Finland we have the government level standardization Katakri that can be used for one part of the requirements but it is for classified information, not directly for cyber ranges, but it has requirements that can be used to understand the situation better.*" (Ed. note: Katakri is National Security Auditing Criteria)

Third interviewee

- [The project] envisioned ISO 9001 as the minimum certification for a joined venture that is managing the federation of cyber ranges. Our initial target is commercial, so 9001 could be sufficient. In case the installation is for government we need to probably ask for 27001 also, but not for a commercial service. Depends generally on who is asking and to what target market you are asking for the federation, but baseline could be 9001. For staff: no requirements, in a case of government, security clearance may be required.

4.4 Optional Questions

Optional questions were asked, if there was time left from the agreed 20 minutes timespan. They did not have any specific focus, as did the obligatory questions, which were weighted towards cyber range federation and certification requirements.

None of the participants had any specific technical requirements for the participants (utilizing the cyber range). The first interviewee stated that they had created cheat sheets for participants to aid them in basic knowledge in Linux and Windows, networking and security topics. The second interviewee said that the exercises or trainings they conduct do no set technical requirements for the participants other than the basic usage of office systems, phones, but "*it depends on the level of the exercise and roles, but in general no special skills is required to participate*". The third interviewee stated from, the [The project] perspective, that there are requirements for the cyber range operators joining the federation "*– – what we want is to give a change to small providers which still may provide some interesting sector specific or niche scenarios, so we try to be agile, of course you need to guarantee a set of minimum requirements in terms of Internet bandwidth, Internet latency and the capacity of your hardware, and the capacity of your staff also, these are fundamental*".

4.4.1 Hybrid Solution – Public Cloud Usage in Cyber Ranges

A Hybrid solution, i.e. one utilizing public cloud services as part of the cyber range was demonstrated, according to two of the interviewees. One interviewee said that it is technically possible, but presently the person did not see any reason to utilize public cloud.

4.4.2 Automated Red Team Workflows

The last optional question, to which all the interviewees were able to answer within the given timeframe, was "*Does you environment include possibility to automate red team workflows, i.e. deploy injects/attacks via a tool?*"

First interviewee

> *First level of automation was created by creating own scripts (for example Wannacry, we automated scripts so that it was automatically launched to the machines or the network), but the tool did not enable to automate red teaming. I have seen that other tools from [other cyber range operator] (company name remove by report editors) are doing it, but our scripts were not able to do this, but it was mandatory for us to have this first level automation and that is why we created scripting. It was done by our own engineering team.*

Second interviewee

> *Yes we do have a comprehensive set of automated red teaming scenarios and attacks done so those can be initiated and therefor done automatically afterwards, or they can be scheduled, so you can say that OK at 1 P.M. certain things start happening by the red team, so yes we do, it is a custom made in-house solution.*

Third interviewee

> *[The Company's] range does include that, we do it, we have a timeline with the possibility to put attacks in certain moments of time, at the moment we have all orchestration work done and some attack scripts, we are enlarging the digital library of attack scripts.*
>
> *From [The Project] perspective I do not know if we can get there, because what we are trying to do is, since we will have a single scenario description language, what we would like is to be able to automatize the conversion between the scenario requested by the customer and then at the end of the negotiation for the service with the cyber range provider, we are envisioning the possibility to automatically implement the service without passing through manual input. So let's say the customer is asking for a phishing kind of service and there is a negation which is going to be supported by the federated cyber range, between the customer and the cyber range provider, at the end both of the parties came to a conclusion, OK that is going to be the service so we will have ten trainee, two trainers and 50 machines, what we would like is to be able to transform the definition of the scenario directly into the infrastructure of the service, internal JSON or XML type of configurations. Ansible may also be needed, almost automatically to build the scenario within the range, I don't know if we will manage to do it in [The Project], probably we manage to do it only with [The Company's] technology cyber range because we have full control and we can already do it, but with our scenario description language, we will see, it would be nice since it would lead to a very fast negotiation between the customer and the provider, but it is complex because there are 10 000 different technologies etc.*

4.4.3 Business Model

The interview timeframe allowed only two interviewees to answer the last optional question "*Do you have a business model to your trainings or exercises, or operate the environment, which you can explain or open up?*"

Second Interviewee

We do have a business model for the training and the exercises, but that is prohibited information (not open information) from many parts, we do have specialists planning, conducting, and analysing the exercises in different roles. That also includes the technical team who are the operators of the cyber range who actually develop and maintain the systems on the infrastructure level, but also inside of the cyber range, the features, bringing up the capabilities. The model is basically that we develop new features all the time in an agile way.

Third Interviewee

[The company] has a business model for the training, we provide cyber ranges in two ways as a service, there you can buy the training service, the R&D service, the testing service (depending on your interest), as a service, we can provide you access to the environment etc. The second option is related to buying license of the cyber range technology itself, then the customer has the possibility to have [the company] managing the service itself in the customer premises, or the customer buys everything and we provide only the maintenance from the software perspective.

Part B: Requirements Specification for Cyber Range Technical Federation

Executive Summary

Part B introduces the requirements specification for the cyber range technical federation applying software defined network (SDN) technology. By implementing technical federation between two or more cyber exercise or training environments, or parts thereof, or labs, the federation may provide a more realistic environment or an environment which contains features and functionalities that a exceeds a single provider's offering without investing to the development of the federated (combined) offering. Customers of technically federated cyber ranges could seamlessly utilize features, services, capabilities and capacity simultaneously from environments located in various geographical areas, even cross-border, without knowing the implementation details. Technical federation of cyber ranges can be established free from the size or complexity of the cyber ranges, the level of realism of those, the domain or use cases the cyber ranges are focused, or the services or functionalities they have. Yet there are some requirements the technical federation must meet and this requirement specification contains production level requirements for SD-WAN federation.

From the end-user perspective, network bandwidth and latency are critical parts in technical federation, in order that their activities can be performed satisfyingly over the public Internet. For example, long network latency creates a visible delay between the letter typed from the end-users keyboard and when it is visually displayed on the screen, thus making the end-user experience poor. The network related requirements defined in this document can be relived, for example when testing the implementation of this specification, but they should be honoured in production kind of environment.

The verification of the requirements is a work scheduled for the year 2021, and the report on this will be delivered in project's deliverable D7.3. The specification is estimated to be used in production at latest in January 2022, where CyberSec4Europe cyber exercise FlagShip 2 is scheduled.

5 Cyber Range Technical Federation

As the terminology related to cyber ranges is evolving, in Part A of this document we proposed a more fine-grained definition for cyber range federation dividing it into Operational Federation and Technical Federation.

Part B of this document covers use cases, use scenarios, connectivity scenarios and requirements for the cyber range technical federation. The target audience of the document are cyber range and network technical specialists. The objective was to define the requirements specification to interconnect cyber ranges over the public Internet. Planned implementation technology was open-source backed software defined wide-area network, SD-WAN, an implementation technology of software defined network (SDN) family. Open-source was a natural selection, when aiming to easily approachable, low-cost solution for wider audience use. SDN approach was selected to enable federation parties to easily modify the federation network, if seen necessary. Based on our own experience, we estimated that SD-WAN could fulfil the requirements of interconnecting cyber ranges over public internet. The requirement specification has been derived from our experience, years of hands-on experience of developing a realistic large live cyber and experiments we have run there, and years of experience of planning, implementing and running cyber security exercises, trainings end education courses, and from CyberSec4Europe survey of existing cyber ranges.

In this document, cyber ranges are specified as either full-scale or small-scale. A small-scale cyber range is focused on providing cyber exercises or trainings for specific small organisations or for single or only a few target environments for cyber exercises, trainings, capture the flag (CTF) competitions, certification, or for cyber security research and development. A full-scale cyber range includes elements of the global Internet (isolated from the real Internet) and multiple simulated organisations or target environments with realistic business and operative functionalities and interconnections between them. A full-scale cyber range may contain the capabilities of one or more small-scale cyber ranges.

Despite the fact that even full-scale cyber ranges are “just” simulation or emulation environments, their network topologies can be highly complex and realistic. The complexity aspect is covered in the document, and it can be used to technically federate both heterogeneous and homogenous cyber ranges.

The use cases, use scenarios and connectivity scenarios, described later in this document, covers topology options to technically interconnect the cyber ranges, technology testbeds or labs. The covered topology options are:

- one-to-one (point-to-point)
- many-to-many (mesh)
- many-to-one (hub)

5.1 Conflict of interest statement

The authors have no conflict of interests regarding to any SD-WAN open-source or commercial technologies, appliances, applications, or companies or corporations benefiting from thereof. Some of the authors of this requirement specification have participated to the development of, operating of, and usage of Realistic Global Cyber Range (RGCE), whilst employed by JAMK University of Applied Sciences, Institute of Information Technology, Finland.

5.2 About the used conventions

To support the interconnection of diverse cyber range network topologies and features, this specification’s convention contains **Specification** and **Checklist** items. The specification items contain independent requirements and they must be interpreted as such. For example, a full-scale cyber range may contain several simulated ISPs connected to each other over simulated Internet, each of the ISPs

could have several customers joining to the simulated Internet, and each customer could have a vast amount of services exposed to the simulated Internet (JYVSECTEC, 2018).

An example of a requirement, independent from any use scenario is the following:

Specification 1.1: MUST have a dedicated Internet connection for a cyber range

An example of a checklist item, which is provided to support the implementation of a specific use scenario is shown below:

Checklist 1.1: Routing Protocols that are Used to Connect Exercise ISPs SHOULD be Agreed Upon

5.3 Use Case 1: Networked Cyber Ranges

The first use case describes how two cyber ranges can be connected to each other in a point-to-point network, or in a mesh-like structure.

The need for various connections arises because the existence of different types of exercises or trainings and because of differences in cyber range structures. Some of the cyber ranges are capable of providing large-scale exercises independently while smaller ranges are capable of providing more dedicated smaller-scale exercises. By connecting smaller ranges together, it becomes possible to enhance the capacity to provide larger-scale exercises or trainings.

This, can for example, include extending the capacity of one cyber range by adding resources or other environments from another range. Additionally, the capabilities of an exercise can be enhanced by connecting multiple cyber ranges together to create one logical cyber range for the exercise. In this document, a logical cyber range is a designated set of interoperable assets (functionalities) and capabilities within one or more ranges interconnected through a secure connection. With this approach, participants in the exercise can connect to the exercise through all cyber ranges that are taking part.

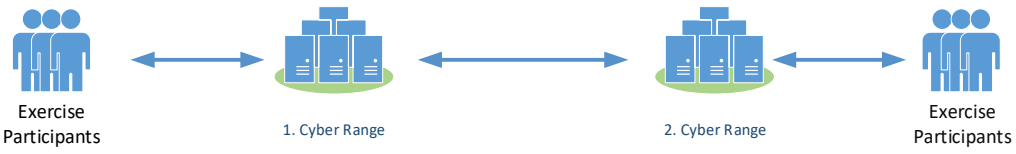

Figure 50: Point-to-Point connection.

The use scenario of point-to-point network as shown in Figure 50 is applicable when there are two ranges forming a single logical cyber exercise environment, i.e., a cyber range. This approach could be considered as a starting point towards more complex technical federation implementations consisting multiple cyber ranges. The size of the cyber ranges, capacity and the level of realism or complicity is irrelevant from the technical point of view.

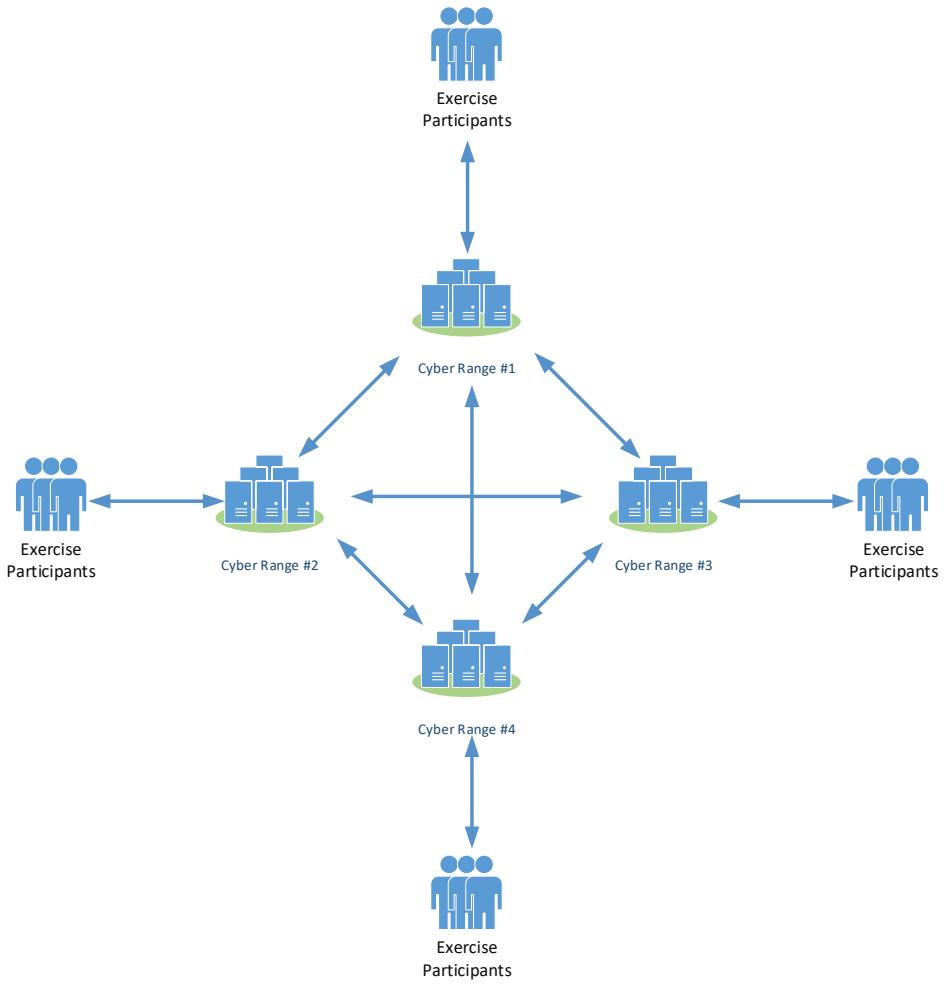

Figure 51: Mesh connection.

Figure 51 shows a use scenario for connecting three or more cyber ranges to each other in a mesh-like or full-mesh manner. This type of connectivity allows for many connections in a full-mesh topology. The formula $n*(n-1)_2$ represents the number of links between n ranges. Depending on the form of the exercise, it might be worthwhile to evaluate critically the need for a full-mesh topology.

5.4 Use Case 2: A Cyber Range as a Hub

In use case 2 the use scenario is one cyber range serving as an exercise provider (a hub) for the exercise.

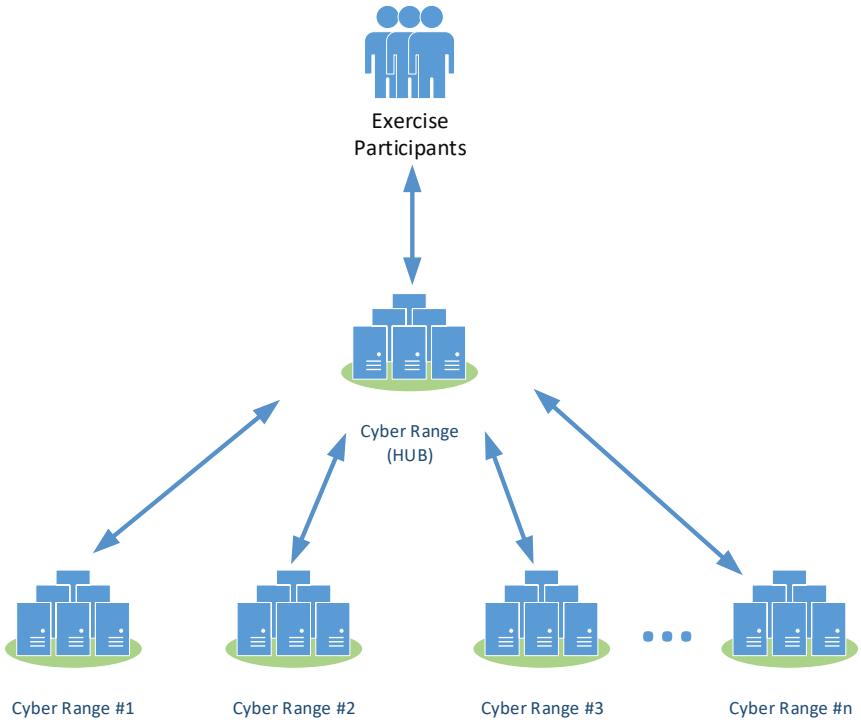

Figure 52: Point-to-multipoint (Hub).

The hub offers connectivity to other cyber ranges that are used for providing additional functionalities to the hub for the exercise. The logical topology for this type of interconnection is point-to-multipoint where all the ranges are connected to one specific cyber range (Figure 52). The hub provides cyber exercises to participants and it adds or enhances the exercises with capabilities from other cyber ranges. In a cyber exercise, all the participants will use the hub range and if they have a need for capabilities from other cyber ranges or labs, they will use those capabilities through the hub range.

5.5 Use Case 3: Adding Testbeds to a Cyber Range

Use case 3 offers the use of domain specificities such as testbeds or labs to provide additional features that are not otherwise available. Testbeds are considered technology-specific testing and experimental environments that do not provide cyber exercises. Testbeds can include technologies such as IoT, ICS, robotics, smart grids, cyber-physical devices, AI, VR/AR, Big Data and healthcare.

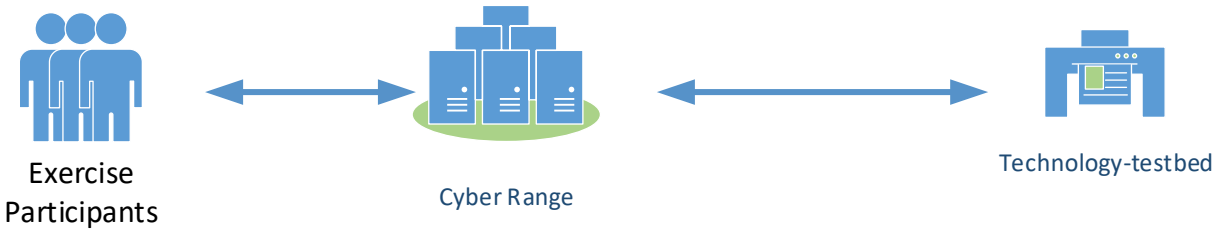

Figure 53: Testbed connection.

These kinds of testbed environments are not often designed for use in cyber exercises, but they can be used as part of the cyber exercises when they are connected to an appropriate cyber range (Figure 53). Connecting testbeds to a cyber range is typically done in a point-to-point connection. Therefore, in a networking perspective the use case 3 is close to use case 1's point-to-point connection between two cyber ranges.

6 Requirements for the Cyber Range Technical Federation

The requirements that are specified in this chapter are for production use. For demonstration and testing purposes these requirements can be lower. For example, for demonstrating technical federation cyber exercise organizations and cyber ranges can use their organization's Internet connection instead of a dedicated Internet connection to the cyber range.

Specifications and checklists in this chapter uses key words that are specified in RFC 2119 to indicate requirements levels. RFC 2119 specifies the following words:

1. MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

5. MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.) (Network Working Group, S. Bradner. IETF, 1997)

6.1 Internet Connection

A cyber range needs an access to the Internet to be able to connect to other cyber range(s). Using the dedicated physical links between cyber ranges (leased-line connection) is not necessarily plausible. Therefore, a cyber range MUST have a connection to the Internet. Using a dedicated Internet connection for a cyber range interconnection provides separation from production networks and is more predictable in terms of bandwidth usage. In modern cyber ranges, many services and activities during the exercise need quite a lot of throughput, which creates needs for the Internet connection to have a reasonable amount of bandwidth available for the cyber range interconnection.

Specification 1.1: MUST have a dedicated Internet connection for a cyber range

Specification 1.2: The minimum bandwidth for the dedicated Internet connection MUST be greater than 100Mbit/s

To be able to have a reasonable quality connection to interconnect cyber ranges the latency to the overlay network, which provides the secure and routed connection between cyber ranges, needs to be as low as possible. The overlay network itself creates some latency and the other cyber ranges connections to the overlay networks interface generate additional latency. Specification 1.3 is for the connection to the cyber range's ISP (Internet service provider)

Specification 1.3: Round-Trip-Time (RTT) to Internet access MUST be less than 25ms

6.2 Overlay Network

Interconnecting multiple cyber ranges for the usage examples described earlier in this document requires a scalable and easily set-up overlay network covering all the participating cyber ranges. The overlay network's function is to create a "virtual" WAN-network for cyber ranges to join which is encrypted and provides appropriate tunnelling functionalities. The overlay network can be implemented as an SD-WAN solution from a commercial ISP or by creating one's own managed SD-WAN (SD-WAN manager) setup. In cyber ranges, the physical or virtualized Customer premises equipment (CPE) makes the connection to the overlay network.

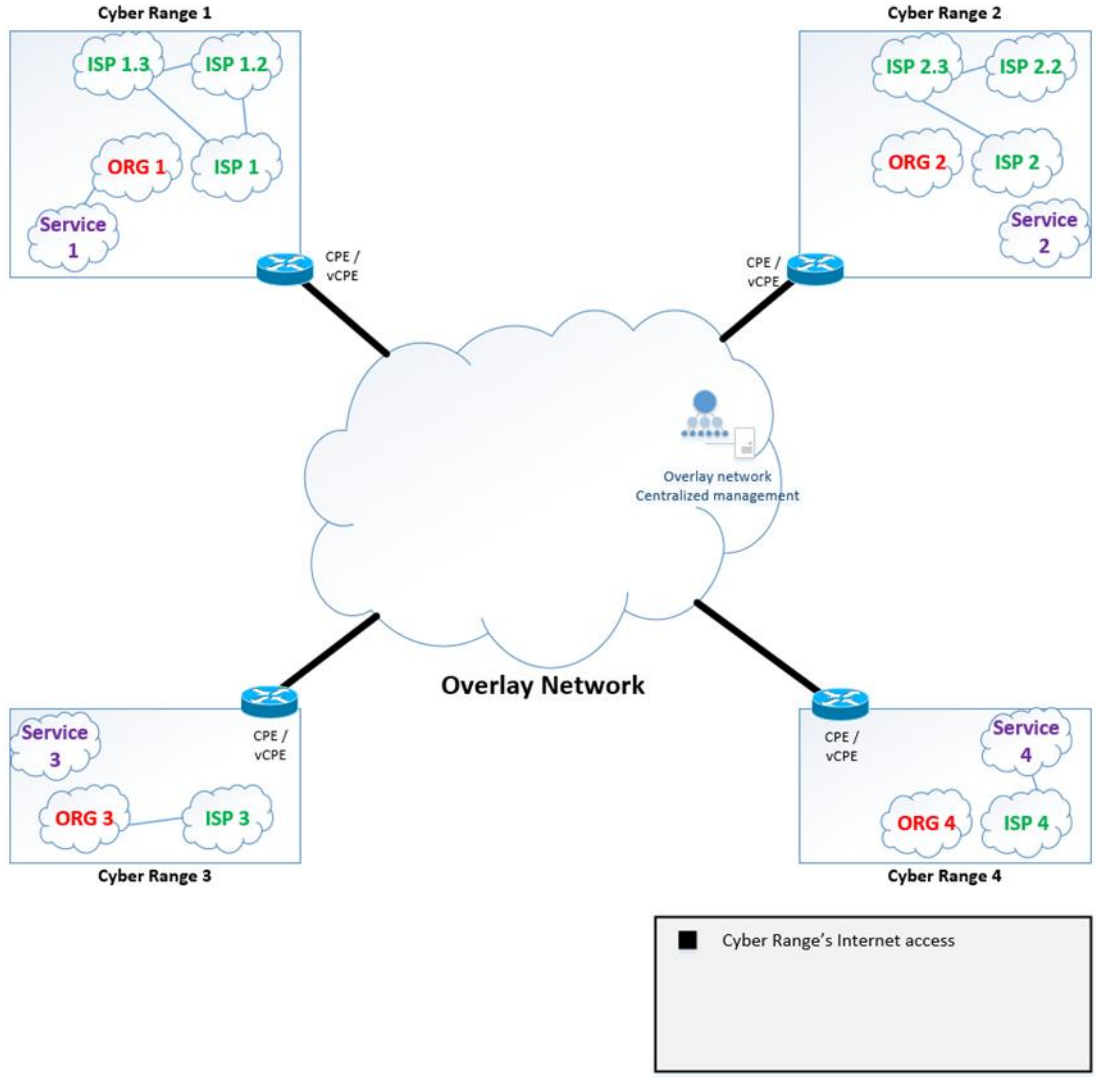

Figure 54: Overlay network.

As shown in Figure 54, each cyber range has its own simulated organizations (ORG[1-4]), there can be more than just one per cyber range), simulated ISPs (usually multiple ISPs per cyber range), and simulate or emulated services (multiple per cyber range). These organizations, ISPs and services are inside the cyber ranges and are normally isolated from the Internet. These organizations can be created for individual exercises or they can be part of the cyber range services. They are connected through the overlay network to a different cyber range. When different kind of services and organizations are connected together, they may need OSI model layer two or layer three connections. For example, if two ISPs are peering with a border gateway protocol together, they need a layer two tunnel between the cyber ranges. On the other hand, the OSI-model's layer three connection is best for some web-services when the client does not have to be in the same layer two network.

Specification 2.1: Overlay network MUST 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)

Cyber ranges are built to mimic the real Internet; therefore, the overlay network must support both IPv4 and IPv6 protocols. If one of these is not supported, the realism and available cyber exercise or training scenarios are reduced.

Specification 2.3: Overlay interface MUST support IPv4 and IPv6 connections in dual-stack

Specification 2.4: Overlay network MUST support IPv4 and IPv6 (cyber range Internet connectivity does not need to be dual-stack)

Earlier in this document, three different use cases were defined for the technical federation of cyber ranges. These use cases defined three different network topologies that the overlay network must support. The three topologies were point-to-point, hub-and-spoke and mesh-like topologies. The Mesh-topology can be divided into two different topologies partial-mesh and full-mesh. Depending on the overlay network the full-mesh can be costlier and take more resources than the partial-mesh. However, in the case of SD-WAN, both of these use the same kind of physical topology, only the logical topology is defined by the SD-WAN portal.

Specification 2.5: Overlay network MUST support the following topologies: point-to-point, hub-and-spoke, partial-mesh and full-mesh

In addition to exercise environments in a cyber range, there exist an Internet access using some kind of customer premises equipment (CPE) that should be either physical or virtualized. With the CPE device cyber ranges connect to the overlay network. Some cyber ranges or testbeds can be behind some firewall or router that is using network address translation (NAT). Those firewalls and router can be owned by a different owner than the owner of the cyber range. In that case, the cyber ranges may not be able to make changes to NAT or disable it, so the CPE device and the overlay network should support connectivity behind NAT. Usually, the SD-WAN Orchestrator does this. The definition of the Internet connection defines that Internet connection's round-trip-time should be less than 25ms to cyber range's ISP. SD-WAN will bring some delay also to the network, however, since SD-WAN can constantly monitor available paths and choose the least congested to route data, SD-WAN can keep the latency low. The maximum end-to-end round-trip-time depends on what kind of data is used in cyber ranges. If all the communications between cyber ranges are done via the overlay network with some real time application, the RTT should be less than 100ms. However, for normal data usage and to console or remote desktop usage less than 200ms is good. These result in the following specifications for the overlay network:

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) MUST be less than 200ms

The overlay network topologies and connections should be managed with centralized management software that can be externally purchased or hosted by some other cyber range. A centralized management software should be available to all cyber ranges that are part of the overlay network.

Specification 2.9: Overlay network must have centralized management to control interconnections between cyber ranges

Specification 2.10: Centralized management should be available to all cyber ranges

When the technical federation is implemented with multiple cyber ranges, there can be more than one concurrent exercise to different customers. It is important that the different customer data is kept separated and the possibility of leakages of information is kept minimal. The operators should be able to make different topologies and networks inside of the overlay network that segregates the concurrent exercises.

Specification 2.11: Overlay network MUST support segregation of concurrent exercises

Because SD-WAN can use the public Internet, it is important that the overlay network is secured and encrypted. When SD-WAN tunnels are encrypted, no one can see the real data even if they eavesdrop the traffic. Encryption must be done with known and well-tested protocols. These result in the following specifications for the overlay network:

Specification 2.12: Overlay network MUST be encrypted using industry standard protocols

6.3 Cyber Range Interconnection

Once the cyber ranges have the interconnection implemented using an overlay network or leased-lines, the different logical connections between the cyber ranges' exercise environments must be agreed upon between the cyber range owners.

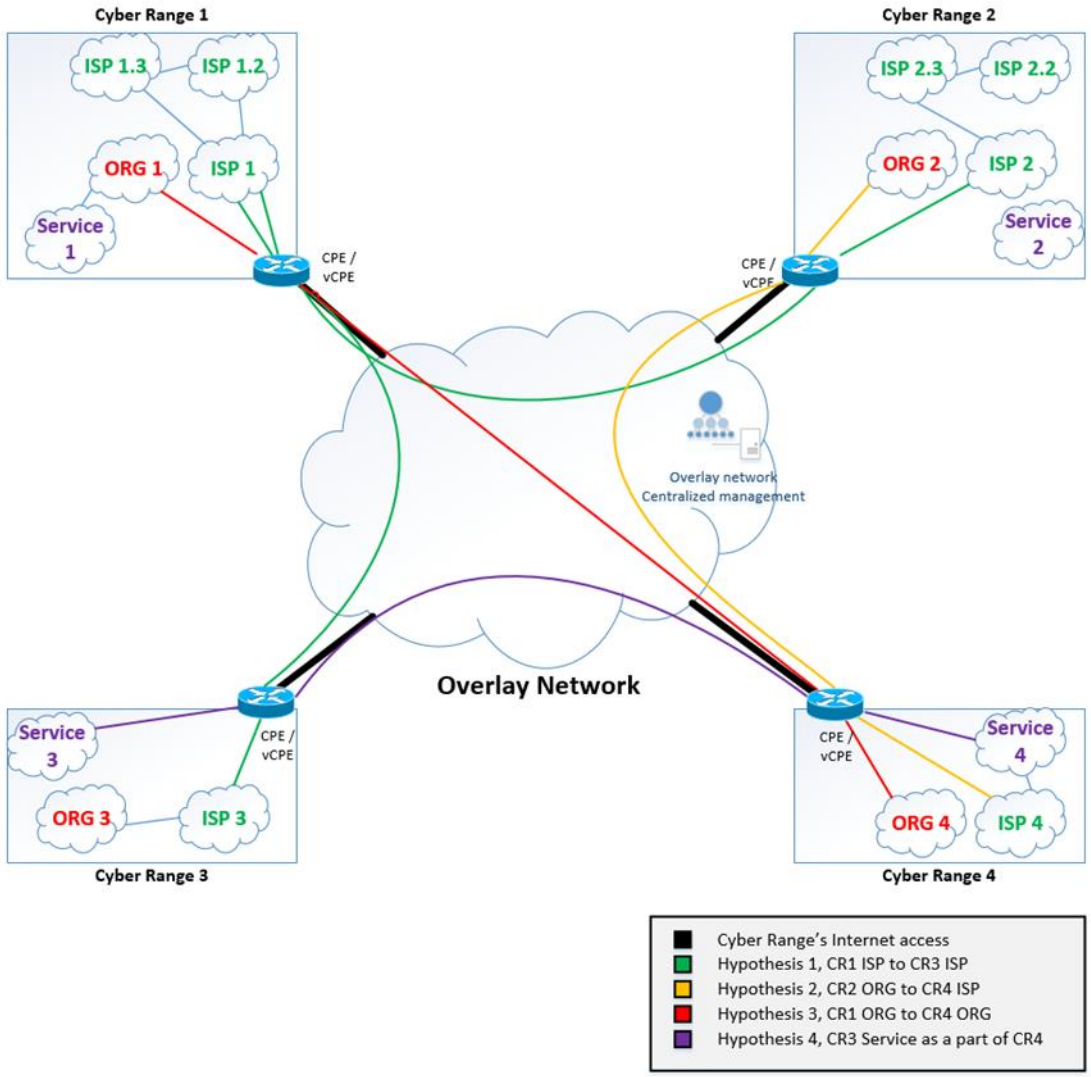

Figure 55: Logical connections.

Figure 55 shows the logical connections between cyber ranges, or part thereof, which might be relevant when creating a joint-exercise between cyber ranges. Cyber range's exercise environments mean fictional or simulated Internet Service Providers (ISP) or organizations that are inside or a part of the cyber range. In this chapter, the term Internet Service Provider (or exercise Internet Service Provider, ISP) or organization (or exercise organization) mean networks that are inside the cyber range.

As shown in Figure 55, there might be an exercise where Cyber Range (CR) 1's Internet Service Provider will be connected to CR2's Internet Service Provider and to the CR3's Internet Service Provider (connectivity scenario 1, green lines). Another possibility is to connect CR2's organization environment to be part of Cyber Range 4's Internet Service Provider (connectivity scenario 2, orange line).

In addition, it is possible to connect the CR1's organization environment to be part of another organization that is in Cyber Range 4 (scenario 3, red line). Another option is also to connect a single device/service to be part of a cyber range, this is scenario 4 (purple line). In the following chapters, checklists that are more detailed are presented per scenario.

6.3.1 Scenario 1: Connecting Multiple Exercise ISPs from Different CRs

Connecting two exercise ISPs together between cyber ranges requires routing. Routing protocols and details should be agreed upon depending on the architecture of the cyber ranges. For example, for BGP connectivity between exercises, ISPs need many configurations to be specified so that the two ISPs can exchange routing information and transmit data.

Checklist 1.1: Routing Protocols that are Used to Connect Exercise ISPs SHOULD be Agreed Upon

An interconnection between two or more exercise ISPs connected on OSI model layer3 level and using Border Gateway Protocol (BGP) routing protocol creates needs to have certain configuration details exchanged between the participating cyber ranges. In addition to mandatory BGP attributes also routing policies and bandwidth limits should be defined. It is possible that cyber ranges can have same IP addresses in use and therefore routing policies must be defined. On those routing policies the IP addresses that are exchanged are defined. The physical bandwidth of the cyber range's Internet connections set limits to the exercise bandwidth. The exercise bandwidth should always be under the Internet connection's bandwidth. This results in the following checklists:

Checklist 1.2: BGP neighbour configuration SHOULD be agreed upon

Checklist 1.2.1: ISP BGP properties SHOULD be specified (Autonomous System number, public IP addresses, ISP name)

Checklist 1.2.2: ISP BGP neighbour IP addresses SHOULD be exchanged between cyber range operators

Checklist 1.2.3: ISP BGP neighbour routing policy SHOULD be defined

Checklist 1.2.4: Numbering schemas SHOULD be evaluated for overlapping IP subnet or AS number

Checklist 1.2.5: Exercise bandwidth between ISPs SHOULD be defined

6.3.2 Scenario 2: Connecting Exercise Organization Environment to the ISP of Another CR

In this scenario, two or more exercise organizations are connected to the exercise ISP of another cyber range based on exercise scenario. This kind of interconnection requires information of exercise organization's technical connectivity to exercise ISP which are the same as in the real world, including IP-addresses and first hop connectivity information. In some cases, the exercise organization requires more than just an Internet access to exercise's "Internet", then the specified architectures and protocols must be agreed on by participating cyber ranges. When the exercise organization only requires Internet access to the exercise's Internet, the following checklists need to be taken into consideration:

Checklist 2.1: First hop connectivity information SHOULD be defined

Checklist 2.2: Bandwidth to ISP SHOULD be defined

Checklist 2.3: Routing from organization perimeter to ISP SHOULD be defined

Checklist 2.4: Organization name and ISP name SHOULD be exchanged

Checklist 2.5: Exercise specific public IP addresses for organization environment SHOULD be defined

In order to use Domain Name System in the exercise organization, the DNS architecture must be defined. The organization needs to know the ISP's DNS servers and the organization has to inform about the DNS delegations to the exercise's ISP. It is also important that both sides of the exercise are in the same time zone, so the Network Time Protocol (NTP) servers must also be defined. These result in the following checklist:

Checklist 2.6: Exercise ISPs infrastructure (DNS servers, NTP, etc.) services SHOULD be exchanged

Checklist 2.7: Exercise organization environment's public DNS architecture SHOULD be defined and the needed DNS delegations should be agreed on

Checklist 2.8: Exercise organization's domain name SHOULD be specified for the exercise

In most cases, cyber ranges are built to mimic the real Internet; therefore, it is important to define also the Public Key Infrastructure (PKI). PKI is used to create certificates for example to websites so a user can see that the webpage is trusted. If the exercise organization wants to get their website or other services to be trusted, they must get their certificates from the cyber range.

Checklist 2.9: The needs of exercise organization public services' PKI-certification SHOULD be defined

However, if the exercise organization has multiple sites, the requirements for exercise ISP connectivity might be more complex and require more detailed information on the connectivity between the exercise organization's sites. This kind of connectivity inside cyber ranges can be implemented in multiple ways, which results the following checklists:

Checklist 2.10: Exercise organization's sites SHOULD be described

Checklist 2.11: Exercise organization's routing policy between its sites SHOULD be defined

Checklist 2.12: Exercise organization's preferred VPN solution SHOULD be described and SHOULD be agreed on

The checklists 2.10 – 2.12 are meant for fictional or simulated organizations that are inside the cyber range. Therefore, the checklist 2.12 "preferred VPN solution" means VPN technology like IPsec used inside the cyber range (not VPN or overlay solution to connect cyber ranges).

6.3.3 Scenario 3: Connecting the Exercise Organization as a Part of Other CR's Exercise Organization

In this scenario, CR1's exercise organization needs to be extended with CR4's exercise organization (see Figure 55). CR4's exercise organization has some functionalities that are needed to connect to CR1's exercise organization. When joining another cyber range's organization, the organization's information has to be about changes between ranges, in including an agreement on IP addresses and if cyber ranges use the same IP addresses, there may be a need for IP address changes or NAT. If the organization uses some kind of domain such as Active Directory, the information needed to join the domain has to be exchanged between ranges. This kind of scenario creates following checklists:

Checklist 3.1: IP address scheme SHOULD be agreed on and defined

Checklist 3.2: Appropriate network configurations SHOULD be specified

Checklist 3.3: Need and method to integrate workstations to Active Directory or equivalent domain SHOULD be defined

Checklist 3.4: In a case of overlapping IP addressing the appropriate NAT design SHOULD be agreed on

6.3.4 Scenario 4: Connecting a Specified Device/ Service as Part of Other CR

In this scenario, CR3's service will used as part of CR4's Cyber Range (see Figure 6). For example, the traffic generator that is owned by CR3 is used in CR4's exercise. In order to connect the device or service to another cyber range, the connectivity information has to be exchanged between cyber ranges. A device or service may need some specific requirements for connectivity to work properly, such as bandwidth and these requirements should be defined. Because the service is owned and administrated in another cyber range, the cyber range that uses the device or service has to know the credentials and instructions in order to use the device or service properly. This creates the following checklists:

Checklist 4.1: First hop connectivity information SHOULD be defined

Checklist 4.2: Bandwidth requirement to first hop SHOULD be defined

Checklist 4.3: Appropriate credentials for the usage of the service SHOULD be provided

Checklist 4.4: In a case of overlapping IP addressing the appropriate NAT design SHOULD be agreed on

Checklist 4.5: Appropriate instructions and technical configurations SHOULD be provided

6.4 Remote End User Connectivity

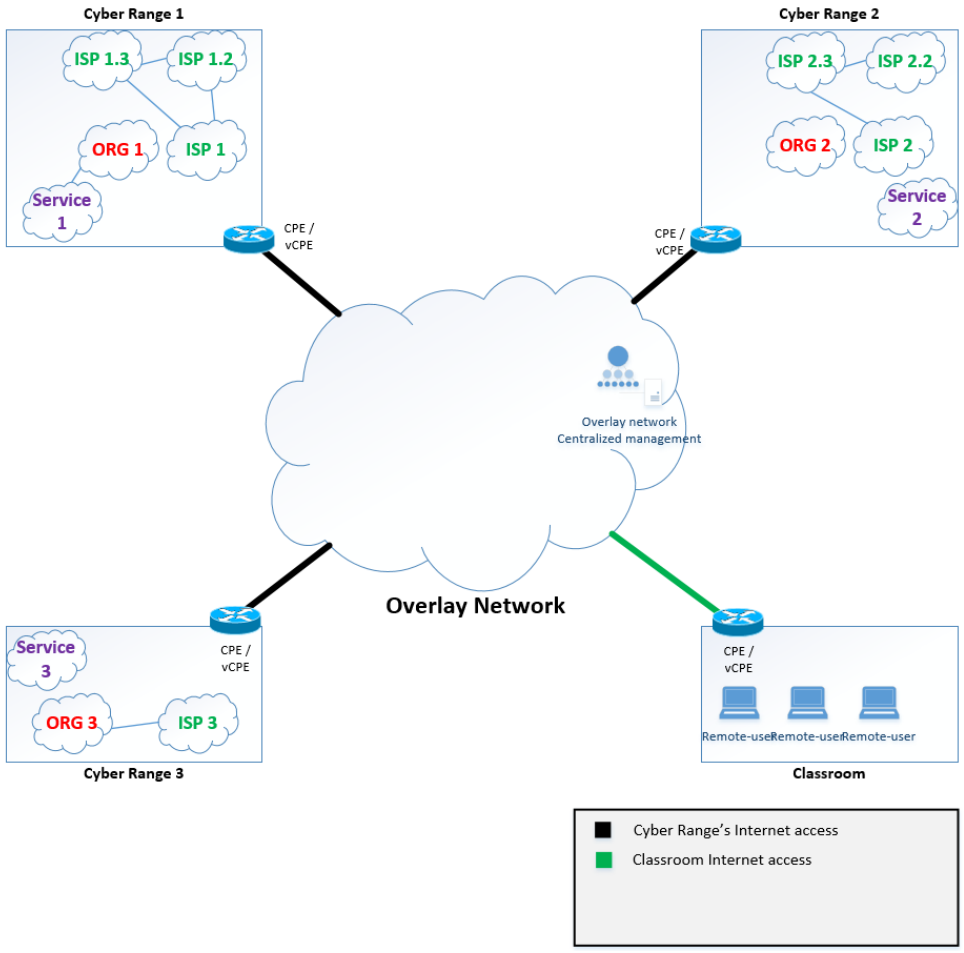

Figure 56: Classroom connection.

In cyber range technical federation, the federation network (overlay) is for the cyber range interconnection and it is not designed for individual end user connectivity. The federation network needs a virtual or a physical CPE device and it will not be feasible to acquire these devices for every end user. However, for a group of remote end users, the federation network can be used for connection of for example one classroom to a cyber range. From the classroom end users can access to the federated cyber range (Figure 56).

6.4.1 Individual Users

For the individual end users some kind of secure connection is needed to access the technically federated cyber range. Normally this connection is done by VPN-connection (Virtual private network).

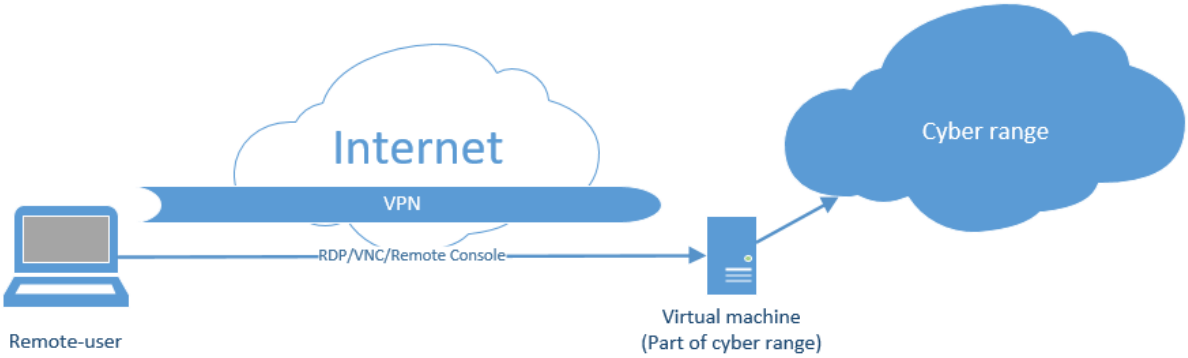

Figure 57: Remote user.

VPN-service (Figure 57) is normally part of the cyber range's services that a cyber range has. There is no standard nor agreement that specifies what kind of VPN cyber ranges should use. That is why cyber ranges offer wide variety of VPN-services to their customers or training participants. In many cases, the VPN connection is for remote access to virtual machine with remote desktop protocol or virtual console.

6.4.2 Requirements

When end users connect directly to the cyber range, some preparations from the cyber range will be required. Before a user can connect to the cyber range, the user needs valid login information from the cyber range. Depending on the level of the exercise and exercise's security or classification level, some form of identification must be done before the login information is given to the user. When the exercise's security requirements allow, simply an invite link to the participants email should be enough. From the invite link the user can register to the cyber range and after the registration, valid login information is sent to user.

Specification 2.41: Cyber range should have a registration portal

Specification 2.42: End user must be identified

Specification 2.43: Cyber range must deliver login information to end user

After the registration, the end user must get the connection instructions. Connection instructions should include download page for VPN client if separated client is needed, connection's technical information (DNS name/IP Address, ports). Because cyber ranges are usually isolated environments, the VPN connection must be full tunnel so all packets will go to the VPN connection and to the destination cyber range and will not go to the Internet. VPN must also provide encryption to connection from the end user to the cyber range.

Specification 2.44: User must have access to VPN client download page

Specification 2.45: Cyber range should provide VPN instructions

Specification 2.46: VPN must be encrypted

Specification 2.47: VPN have must be full tunnel

6.4.3 Challenges

Cyber ranges include many different services that are for maintaining the cyber range, its infrastructure or part of cyber range's functionalities. Some of these services/products are bought from commercial vendors and these include also licensing of the product. Normally vendors have different licensing for local and remote usage. Many vendors licensing the remote usage as a service provider license. This means that if cyber range has only bought normal licences it cannot legally offer commercial products to remote users before it updates needed licences. Service provider licences are normally also more expensive than local usage licences.

7 Conclusions

This chapter introduces the conclusions of our research. Chapters from 7.1 to 7.5 are based on the findings of the survey and chapters 7.6 to 7.8 on the findings of the interviews, all together referring to Part A of this document. Chapter 7.9 concludes Part B of this document. Lessons learned and recommendations for future work is discussed in chapter 7.10.

Overall, the terminology of cyber security in the context of cyber ranges is a work in progress. During writing this report, this was well noticed in the discussions and interviews. In addition, two out of three interviewees specifically stated that there is need to define taxonomy for the domain. Currently the confusion may be due that cyber ranges are actively developed and researched and used broadly in different contexts (Figure 13).

One future direction is to work on taxonomy and ontology related to cyber ranges. The work should include cyber range vendors, service providers and operators, which offer various cyber exercise or training services to different target groups (Figure 14), and representatives of clients and customers, so the broad spectrum of use cases, needs and requirements would be taken into account.

7.1 Background

Majority of the respondents were from large companies/ organizations spread quite evenly across Europe, North Europe slightly dominating. Most organizations were cyber range providers, operators or consultants some of these were in addition using a cyber range as an attendee or participant. The cyber range in question was already in use in most cases, whilst the rest of the cyber ranges were under planning. According to the respondents (Figure 6, Figure 7), most have a self-hosted and self-operated cyber range, more commercial solution was also used, by having SaaS or IaaS solution, but operating it by themselves. In addition, pure commercial or outsourced solution was also reported.

Most organisations have less than ten cyber range professionals and cyber exercise professionals (Figure 1, Figure 9, Figure 10). Typically, they were reported to spend a few days configuring the environment for a cyber exercise or training (Figure 11).

Minority of the respondents stated that their environment contains both dynamic and static elements, but majority responded having dynamic elements, meaning the environment is customised according to the needs of the exercising party (and exercise objectives Ed. note) (Figure 12).

The five most chosen primary uses cases of cyber range (Figure 13) were security education, security research and development, competence building, development of cyber capabilities, and in the fifth position were both security testing and certification, and national and international cyber exercises.

Top three primary target groups were companies and enterprises, government organisations and degree level students (Figure 14). It was also reported that training service providers are in focus. Participant roles in Figure 15 and the reported free form text shows that cyber security professionals and researchers

are the two most popular primary target groups of participants. Also, it was reported that business representatives, employees, and different roles from an organisation are primary target groups.

The reported cyber ranges offer a variety of different environment for participants (Figure 14), three most common being general critical infrastructure, IoT and Scada systems. Also, general ICT infrastructure, private cloud, Software development (for supply chains), ICT service providers (ISP & cloud providers) environments were available for participants.

Only rare organisations which provide cyber ranges or related services use cyber ranges themselves. This finding is a bit odd, as the results of reported participant roles had listed the technically skilled employees and other roles required in incident response. In addition, available environments indicate the cyber ranges have the capability and capacity to accommodate selected parts of the organisations to exercise with the business.

Many of the cyber ranges have no support for real or exercise-only, i.e. simultaneous, organisations in a single and shared training session. However, there are cyber ranges that support multiple organisations (Figure 19). It was reported that the number of simultaneous training sessions varies from single session to ten or more sessions (Figure 20). Majority of participants in a training was reported to be less than 30 persons (Figure 21). Most of the cyber ranges were remotely accessible, but there were also cases where the individuals are required to run the environment or parts of it in their personal equipment (Figure 22). Training duration was usually one day or less (Figure 27). Together these indicate that majority of the cyber ranges were focused to develop individuals' skills and knowledge. There are indicators that some the cyber ranges can conduct large scale live cyber exercises for companies or organisations and their service providers, which is those operate in real world. Sessions targeted for individuals are typically shorter in duration than conducting a cyber exercise for a company or organisation.

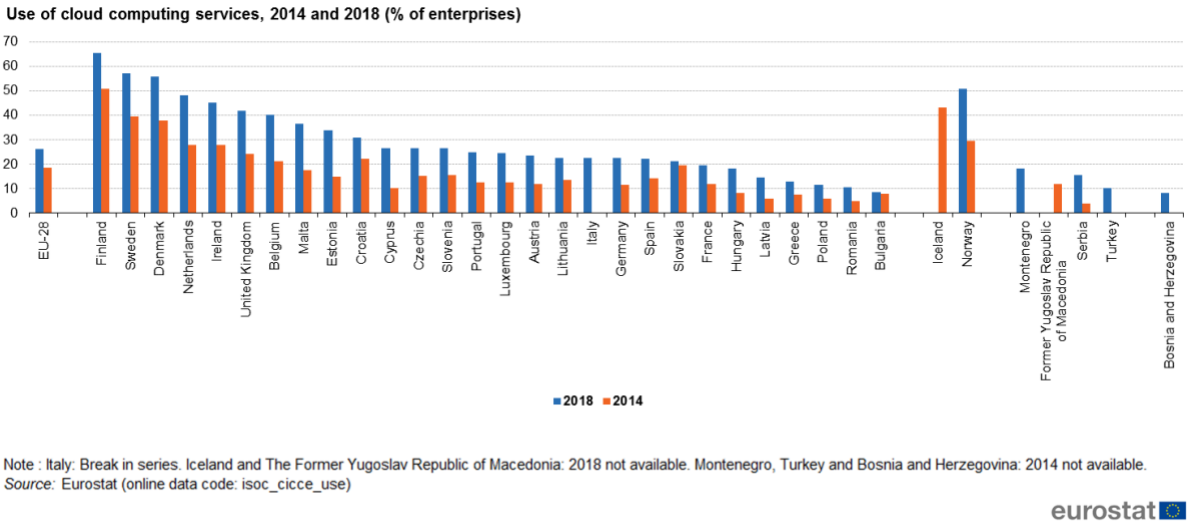

Figure 58: Usage of cloud computing services in Europe 2014-2018.

Eurostat (Eurostat, 2018) reports that the use of cloud computing services in enterprises has increased European-wide. In the enterprises of EU's member states the use has increased from 19% (2014) to 26% (2018) (Figure 1Figure 58). The most common acquired services were e-mail (18%) and storage of files (18%). Future research should highlight whether or not cyber ranges have followed the trend of cloud service usage in order to provide simulated or real cloud services as part of their training environments.

7.2 Performance Reporting of cyber range attendees

Cyber range individual users receive performance reporting in the majority of the responses (Figure 24). The report they receive is generated automatically, manually or a verbal report is given. There were answers that no report of any kind is given, or the performance reporting is not applicable (in some use cases Ed. note).

Cyber exercises or trainings may contain teams, either actual or simulated, i.e., session specific. In majority of responses a report is given. However, for teams the most common was manually generated report, followed by automatically generated and verbal performance report (Figure 25).

7.3 Cyber Range Technical Specification

Before entering to technical questions, the respondents were asked if they were in the position to answer technical questions. 23 answered that they were in such position (N=38), Figure 29.

Identity and Access management was the first technical topic, it was asked if the cyber range respondents were referring to had single-sign on or centralized user management service for participants (Figure 30). Depending on the primary use case of the cyber range in an exercise or training session, centralized access management or single sign-on gives benefit for participants in terms of realism as many organizations and companies utilize such services. Highly productised trainings or exercises, utilizing static configuration, where same training content are run repeatedly to changing participants, single sign-on or centralized user management may be a curiosity without much benefit for the conductor or participant. Such trainings are well suited for capture the flag (CTF) kind of trainings, competitions or training individuals for developing their technical skills and knowhow. Larger cyber ranges may have multiple centralised user management services for large scale exercises and trainings.

The survey included a question on number of networks in the cyber range, both IPv4 and IPv6 were asked (Figure 31). The survey respondents had a large number of networks in their environment, single most selected option for both IPv4 (N=21) and IPv6 (N=22) was over 100 networks. The number of networks can be seen as one indicator of the realism of a cyber range, but depending on the use case and the objectives of a cyber exercise or training, even a small number of IPv4 or IPv6 networks may well offer the required environment to achieve the objectives.

The Border Gateway Protocol (BGP) is used by the Internet to route traffic. The existence and the number of BGP autonomous Systems (AS) indicates the level of realism of the simulated Internet in a cyber range: the higher number of autonomous systems, the more realistic Internet-like environment. From Figure 32 it is seen that the options “none” and “I don’t know” dominate and only nine respondents indicate having BGPs. According to APNIC, in January 2020 there were 66 800 AS in the Internet, the annual growth being 6% since 2017 (APNIC, 2020). The level of realism on simulating the Internet is not limited to the BGP AS number, but it is also vital to ask other features that are used to replicate Internet level services (e.g. DNS hierarchy).

The technical capacity, i.e., RAM, GHz of CPUs, Disk capacity of cyber ranges reveals interesting information. The most common selection of RAM capacity (Figure 34) was that eight cyber ranges have over 1000 Gb, that is over 1 TB of RAM. The results in general indicate that there are highly capacitive cyber ranges in terms of RAM available. In question querying total CPU GHz available in the environment (Figure 35), most selected option was “1000 GHz or more”, which is over 1 THz of raw processor power. The results of this question strengthens the impression of existence of technically high capacity environments, running workloads which require processor power, but also indicating that there are environments which use lightweight solutions that require relatively little processor power but are in demand of RAM. Total disk capacity was asked in TB units (Figure 36). Most common choice by the respondents was “*Less than 100 TB*”. The responses seem to be in align with each other in terms of total

RAM, CPU and Disk capacity, even though the measurement unit was switched, RAM and CPU were Giga but Disk capacity was Tera.

From the above results, one can conclude that large organisations, with 500 or more employees, have cyber ranges with technological capacity and capability to offer services, yet there exist well-specialized cyber range vendors also in organisations with less than 249 and less than 50 employees.

Yamin, Katt & Gkioulous discus that virtualization by SDN and container technologies may bring the required scalability in the transition from class-room oriented testbeds to run time environments close to the real world (Yamin, Katt, & Gkioulos, 2019). In the survey, virtualisation was covered by two questions, one was "*Number of virtual machines in the environment"* (Figure 37), the other one was the SD-WAN option inside the question "*Selected the integration / federation technologies you have used or are planning to use*" (Figure 43, Figure 44). There was no correlation with organisation size and the integration or federation technologies (Figure 43). It is seen from the results that in terms of virtual machines, there exist large (over 1000) and medium sized (less than 1000, but over 100) cyber ranges available. It should be noted, that the classification of the cyber range sizes, i.e. large, medium or other, is not formally established. Also, it should be noted that the number of virtual machines does not directly correlate with the realism of the cyber range.

The majority of the cyber ranges did not provide any speed variance between the networks. For a realistic cyber range, the networks speed variance is needed, as it occurs in real-life between ISPs, office networks and even in operational networks. It should be noted that for some cyber range use cases the speed variation of network is optional.

The evaluated cyber ranges fulfil the ECSO definition of a cyber range. Some may offer the realism of a real-world (Internet-connected) use environment. To determine if a cyber range is *realistic enough*, one should start with the planned use case and its objectives, determine the needs and requirements they put for the cyber range, and compare them with the cyber range's features, capabilities resources and capacity. It should be critically evaluated if a missing feature, capability, resource, or lack of capacity jeopardizes the achievement of the objectives of a use case.

Determining *if a cyber range is realistic*, one should consider several aspects of the cyber range. They include, but are not limited to the adopted technologies, the existence of simulated global Internet services as discussed earlier in this report, the interdependencies between simulated services and service providers, and the simulated user traffic (i.e. noise). A realistic cyber range enables a broad spectrum of scenarios involving e.g. darknet, cryptocurrencies and other block chain technologies, capabilities and features for red team adversary performing various attacks and injects, e.g. BGP hijacking in a cyber exercise. The maximum number of organisations and the number of participants in a cyber exercise or training session should reflect real-world situations: rarely are companies or organisations self-sufficient operating their ICT environment or doing first response to a cyber incident and performing mitigation activities, therefore the cyber range should be able to accommodate the service providers also.

A realistic cyber range also provides the environment for cyber security research, testing and even certification for researchers, developers, companies and organisations which have been given cyber security requirements. For example, the ANSI/CAN/UL standard 2900-2-1:2018 defines software security requirements for network connectable components of healthcare and wellness systems. It explicitly states that such components shall be tested against known vulnerabilities, malware, malformed inputs, and structured penetration testing shall also be conducted. Organisations facing such requirements may benefit by using a realistic cyber range for running and completing the required certification process.

Given the number of cyber ranges professionals (Figure 8), the number of cyber exercise professionals (Figure 10) and comparing them to the existing technical capabilities described earlier in this chapter, one may only estimate the demand of these professionals in current job markets.

7.4 Cyber Range Federation

As the term cyber range federation is non-stable, we have proposed a more fine-grained definition, i.e. we divided it to Operational Federation (OF) and Technical Federation (TF). OF could be defined as sharing a cyber exercise´s operational and technical data in machine readable form even if the cyber ranges are not interconnected or integrated, as stated by ECSO (ECSO, 2020). Russo et al have introduced CRACK framework and CRACK SDL (Russo, Gabriele, & Alessandro, 2020), a scenario definition language, which together may fulfil the definition of OF. The de facto commonplace federated services, offered by third-parties, are available on-demand for the end-user, with no additional activities but his/her authentication, given the trust-relationship between the end-user home organization and the service provider has been established. Therefore, we propose that Technical Federation is defined as agreeing between federation parties on how they can utilize or consume specified functionalities, services, capabilities or resources from other parties of the federation and implementing them together. Neither TF or OF require one another to be implemented or deployed.

7.5 Cyber Range Connectivity

Cyber range connectivity is required for technical federation or integration. From the perspective of an end user, the speed to public Internet and network latency are aspects that affects to the experienced quality of an interconnected cyber range or to a cyber exercise or training itself - even other (technical) arrangements or exercise scenarios would be excellent.

The majority of the cyber ranges were reported to have dedicated Internet connections, followed by equal answers for options that it has been planned and there was no dedicated Internet connection. The majority of the cyber ranges had a connectivity speed of 100 Mb/s. The connectivity speed may well suitable for the cyber range use cases, even though modern consumer grade fixed-line connectivity options offer higher network speeds. The reported latency of the cyber ranges were under 75 ms. The connectivity is discussed as a first requirement in PART B, chapter 6.1 Internet Connection.

7.6 Operational Federation (OF) and Technical Federation (TF)

Interviews were made with respondents who gave their permission for it and had indicated that they have done federation of cyber ranges (see Chapter 4). From the interviews it was seen that there were benefits from OF via sharing scenarios and virtual machines between the several standalone (i.e. non-interconnected) cyber ranges of a company. This had also benefits of spreading know-how and skills of cyber range operators and cyber exercise planners and conductors. On the other hand, it was seen that OF in multi-party commercial business is an unsolved challenge in terms of governance, financial and eventually in technical perspective. Concerning governance, a question was raised on how to ensure that originators receive business benefit i.e. financial reward from sharing scenarios or virtual machines, which their staff have spent work hours, “sometimes a lot”. In addition, it was mentioned that eventually OF becomes a technical matter, as the scenarios or virtual machines set technical requirements, which the technical cyber range environment should, but may not be able to fulfil. As an example, a large scale realistic cyber exercise, which requires a large cyber range and corresponding networked infrastructure behind it, has such scenarios that cannot be run in a small-scale cyber range or test lab. Russo et al. have introduced CRACK framework and CRACK SDL (Russo, Gabriele, & Alessandro, 2020), a scenario definition language, which together may fulfil the definition of OF, but this needs more research and investigation.

Technical Federation (TF) was seen beneficial to scale-up features and capabilities of existing cyber range(s) when conducting a cyber exercise, the cyber exercise also benefits from a niche environment available elsewhere, and it was mentioned that technical federation is an enabler technology when conducting multinational cyber exercises between several sites in several countries. The need of TF is

evaluated case by case, when the cyber range operating is a large full-scale live cyber range, with rare need to use features or capabilities from external parties.

7.7 Certification Requirements of Cyber Ranges

The interviewees were asked if they had certification requirements for the environment they referred, for the facilities in which the environment is operated, or the staff operating or accessing the environment. Also, it was asked, if they could share the standard they are referring to. ISO 9001 was mentioned as a vision for the minimum certification requirement. It was also mentioned that there are no obligatory certification requirements at the moment. Still the results indicate that there is a need for recognized certification requirements for cyber ranges especially since the term cyber range can still be understood differently. It was seen that recognized certification requirements could help to create common understanding, taxonomy, and language when spoken of cyber ranges.

7.8 Additional Remarks on the Interviews

Hybrid solutions, i.e. utilizing public cloud services as part of the cyber range, were mentioned, but one interviewee said that even though it is technically possible, the person did not see a reason to utilize public cloud at the moment. The interview did not have a follow-up question on how the interviewee has arranged the simulation of public cloud services if they do not use public cloud. It would have been interesting to hear this from a cyber exercise or training attendee perspective.

Automating red team workflows was at a different stage for all interviewees, and the stages were:

- done with a comprehensive set of automated red teaming scenarios
- all orchestration work done and some attack scripts, at the moment enlarging the digital library of attack scripts
- at a stage of first level automation with own scripts
- ECHO perspective: a single scenario description language seen more important at this stage

From the business model perspective not much was revealed, but it was said that there is a business model for the training and the exercises, there are specialists planning, conducting, and analysing the exercises in different roles. On the other hand, it was stated that cyber ranges are provided in two ways as a service, or by buying license of the cyber range technology itself.

7.9 Requirements for the Technical Federation of Cyber Ranges

The requirement specification introduced in Part B describes three use-cases for cyber range technical federation, i.e. sharing features, services, capabilities and resources between two or more cyber ranges. It also introduces requirement specification following RFC 2119 notation. The requirement specification is targeted using open-source SD-WAN technology to technically federate cyber ranges, and it describes four federation scenarios for federation. Intentionally it does not discuss the circumstances when a scenario should be applied. The verification of the requirement specification will be documented in project's deliverable D7.3, which is scheduled for publication in August 2021.

7.10 Lessons Learned and Recommendations for Future Work

From the collected data it was not possible to draw a prioritized list of primary use cases nor of target groups. The duration of the planning of the exercise or training session was not included in the questions. For future research, these should be taken into account to better understand how the cyber ranges are used and what kind of work effort is required before, during and after an exercise or training. Also, it could be enquired the existence and technology how simulated user traffic (i.e. noise) is generated in

cyber ranges. Using noise traffic and the method it is generated are indicators of the realism of a cyber range.

An exact number of autonomous systems was not asked in the survey; this issue should be added in a future survey to give a more specified and clear view on the matter. A future direction for cyber ranges, depending on their users use-cases and customer needs and requirements, could be to research implementing BGP AS in their environment, or collaborate with cyber ranges that have those already in place to offer a realistic Internet-like environment. As already mentioned (in 7.3.) the level of realism on simulating the Internet is not limited to the number of BGP ASs, but it is also vital to ask other features that are used to replicate Internet level services (e.g. DNS hierarchy).

The survey did not include a question on the use of virtualization technologies, virtualized or bare-metal operating systems, nor on the computing power of the Graphics Processing Units (GPU). Also missing was the used business model of cyber ranges. These could be added in a future research to better understand the current technologies used in cyber ranges and the business model used.

The SD-WAN option was selected by four respondents (Figure 35). It may be that the respondents use container technology, which includes orchestration and management of networks, which fulfils the current need and requirements, moving the adoption of SDN technologies to later times. However, this cannot be directly drawn from the survey, but should be investigated in a future research.

The survey did not make distinction between live, i.e. running, and powered-off, i.e. on-rest virtual machines. A future research could try to better understand whether there exist any differences between live and powered-off virtual machines and cover the used container technologies and the usage of the features and capabilities they offer. For taxonomy development we propose discussing and agreeing on the size classification of cyber ranges.

The conducted survey shows that the majority of the respondents are planning to do cyber range federation or integration (Figure 42), whereas five respondents answered that they already have done it. At the survey stage, a definition of cyber range federation or integration was not provided, so a future research objective should be to better understand what exactly the plans are, would they be technical federation, operational federation, or integration. This also highlights the need for defining a cyber range taxonomy.

8 References

APNIC. (2020, January 14). *BGP in 2019 – The BGP Table*. Retrieved June 29, 2020, from Regional Internet Registry administering IP addresses for the Asia Pacific: https://blog.apnic.net/2019/01/16/bgp-in-2018-the-bgp-table/

ECSO. (2020, March 30). Understanding Cyber Ranges: From Hype to Reality. Retrieved May 4, 2020, from https://ecs-org.eu/press-releases/understanding-cyber-ranges-from-hype-to-reality

Enisa. (2019, February). *ENISA Good practices for IoT and Smart Infrastructures tool.* Retrieved July 07, 2020, from Internet of Things (IoT): https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/iot-tool-how-to-guide

European Defence Agency (EDA). (2019, November 07). *EDA Cyber Ranges Federation project showcased at demo exercise in Finland*. Retrieved June 18, 2020, from European Defence Agency: 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

Eurostat. (2018, December). *Cloud computing - statistics on the use by enterprises*. Retrieved June 29, 2020, from https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights

Eurostat. (2020, April). *Number of enterprises by enterprise size class, 2017*. Retrieved 07 24, 2020, from Structural business statistics overview: https://ec.europa.eu/eurostat/statistics-explained/index.php/Structural_business_statistics_overview

JYVSECTEC. (2018). *Cyber Range*. Retrieved June 23, 2020, from JYVSECTEC - Jyväskylä Security Technology: https://jyvsectec.fi/wp-content/uploads/2018/10/JYVSECTEC-cyber-range.pdf

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019). "Pedagogical Aspects of Cyber Security Exercises. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 103-108). Stockholm, Sweden: IEEE. doi:0.1109/EuroSPW.2019.00018

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019). Pedagogical Aspects of Cyber Security Exercises. *IEEE Conference Publications; IEEE Xplore*. Stockholm, Sweden: IEEE. doi:10.1109/EuroSPW.2019.00018

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019). Pedagogical Aspects of Cyber Security Exercises. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 103-108). Stockholm, Sweden: IEEE. doi:0.1109/EuroSPW.2019.00018

Kurze, T. &., Kurze, T., Klems, M., Bermbach, D., Lenk, A., Tai, S., & Kunze, M. (2011). Cloud federation. *CLOUD COMPUTING 2011* (pp. 32-38). Rome, Italy: IARIA. Retrieved July 8, 2020, from https://www.thinkmind.org/download.php?articleid=cloud_computing_2011_2_20_20114

Ministry of Defence of Finland. (2019, November 11). *EDA Cyber Ranges Federation project showcased at demo exercise in Finland*. Retrieved 07 09, 2020, from Ministry of Defence: https://www.defmin.fi/en/topical/press_releases/2019/eda_cyber_ranges_federation_project_showcased_at_demo_exercise_in_finland.10065.news

Network Working Group, S. Bradner. IETF. (1997, 03). *Key words for use in RFCs to Indicate Requirement Levels.* Retrieved April 29, 2020, from https://www.ietf.org/rfc/rfc2119.txt

Reini, H. (2019, November 4). *CYBER RANGES FEDERATION – TOWARDS BETTER CYBER CAPABILITIES THROUGH COOPERATION*. Retrieved June 18, 2020, from Finland's Presidency of the COuncil of the European Union: https://eu2019.fi/en/article/-/asset_publisher/cyber-ranges-federation-yhteistyolla-kohti-parempaa-kyberkyvykkyytta

Russo, E., Gabriele, C., & Alessandro, A. (2020). Building Next Generation Cyber Ranges with CRACK. *Computers & Security Volume 95*. doi:10.1016/j.cose.2020.101837

Saharinen, K., Karjalainen, M., & 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)* (pp. 3-7). New York, NY, USA: Association for Computing Machinery. doi:10.1145/3369255.3369266

Vykopal, J., Ošlejšek, R., Celeda, P., Vizváry, M., & Tovarňák, D. (2017). KYPO Cyber Range: Design and Use Cases. *12th International Conference on Software Technologies* (pp. 310-321). Madrid, Spain: SciTePress. doi:10.5220/0006428203100321

Yamin, M. M., Katt, B., & Gkioulos, V. (2019, Janurary). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*. doi:10.1016/j.cose.2019.101636

Annex A: Survey form

Question types: Multiple choice, Check box, Textfield

1 Amount of personnel in my organization

- Less than 10
- Less than 50
- Less than 249
- Less than 500
- 500 or more

2 Country of my organization's HQ

- Select box (all countries)

3 Role of cyber range in our organisation

- Using cyber range as an attendee / participant
- Cyber range provider / operator / consultant

4 Current status of using cyber ranges

- Is using
- Is planning
- Is not using nor planning

5 Cyber range hosting type

- Self-hosted & self operated
- SaaS / IaaS but self operated
- Commercial / outsourced

6 Additional information about existing or planned cyber range

- 6.1 Name of cyber range
- 6.2 Cyber range operator or vendor
- 6.3 Contact information for cyber range (e.g. URL, email)

7 Number of cyber range professionals

- None
- Less than 4 persons
- Less than 10 persons
- Less than 30 persons
- 30 persons or more
- I don't know

8 Number of cyber range exercise professionals

- None

Less than 4 persons

Less than 10 persons

Less than 30 persons

30 persons or more

9 How many working hours do you typically use for configuring the cyber range for a specific use case?

a few hours or less

about a day

a few days

more than a week

more than two weeks

10 Characteristics of cyber range(s)

Static configuration (No customized environment or the customization is limited)

Dynamic configuration (Environment is customized according to attendees needs)

11 Primary use case of the cyber range(s)

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

National and International Cybersecurity Exercises

12 Primary target groups of the cyber range(s)

General public

Secondary level students

Degree program students (Bachelor or Master's degree students)

Government organizations

Companies and Enterprises

Non-profit associations or similar

Other

13 Primary participant roles of the cyber range(s)

Director (Business, Director, Communication, etc.)

Developer

Researcher

Security professional

Educator

Other

14 Environments available for training

General critical infrastructure : Electricity, Heat, Water, Sewage

Infrastructure: Maritime, Space, Land transport

Cyber Physical Systems (CPS)

Healthcare

IoT

Mobile infrastructure (e.g. 4G, 5G, GSM, WIMAX)

Robotics

SCADA

Smart-Grid

Unmanned Aerial Vehicles (UAVs)

Other

15 Participant and organizational capacity - Number of simultaneous organizations or environments in a single and shared training session. An organization may be an existing one, or fictional

None, no organizations either fictional or actual are used

Less than 3 organizations

Less than 5 organizations

Less than 10 organizations

10 organizations or more

16 Participant and organizational capacity - Number of simultaneous but distinct training sessions, e.g. same content but different organizations training

We can run a single session at a time

Less than 5 sessions

Less than 10 sessions

10 sessions or more

17 Participant and organizational capacity - Maximum number of persons in a training session

Less than 10 persons

Less than 30 persons

Less than 50 persons

Less than 100 persons

100 persons or more

18 Primary access method of the cyber range

Personal computing equipment, e.g. the environment runs on a laptop or virtual machine(s) on it

Remotely accessible (e.g. cloud)

On-site / on-premises

19 Performance reporting

19.1 Does an individual participant receive a performance report?

Yes - an automatically generated report is given

Yes - a manually generated report is given

Yes - a verbal report is given

No performance report is given

N/A - not applicable

19.2 If there are teams (simulated or real) attending to an event, will they receive a performance report?

Yes - an automatically generated report is given

Yes - a manually generated report is given

Yes - a verbal report is given

No performance report is given

N/A - not applicable

19.3 If there are organizations (simulated or real) attending to an event, will they receive a performance report?

Yes - an automatically generated report is given

Yes - a manually generated report is given

Yes - a verbal report is given

No performance report is given

N/A - not applicable

20 Training duration

2-3 hours

One day

A work week or less

More than a work week

21 Are you in the position of answering to technical questions related to the cyber range you are referring to?

Yes

No

22 Identity and Access Management - The environment has single-sign-on or centralized user management service for participants

Yes

Partial

No

23 Technical capability - Networks

23.1 Number of IPv4 Subnets (/8 /16 /24), either public or private

Less than 10

More than 10

More than 50

More than 100

I don't know

23.2 Number of IPv6 Subnets (/64), either public or private

Less than 10

More than 10

More than 50

More than 100

I don't know

24 Technical capability - Networks - Number of Border Gateway Protocol (BGP) autonomous systems (AS)

None

Less than 10

10 or more

I don't know

25 Total RAM available in the environment

Less than 50 Gb

Less than 100 Gb

Less than 500 Gb

Less than 1000 Gb

1000 Gb or more

I don't know

26 Total CPU GHz available in the environment

Less than 100 GHz

Less than 500 GHz

Less than 1000 GHz

1000 GHz or more

27 Total disk capacity available in the environment

Less than 5 TB

Less than 100 TB

Less than 500 TB

Less than 1000 TB

1000 TB or more

28 Amount of virtual machines in the environment

Less than 30 virtual machines

Less than 100 virtual machines

Less than 500 virtual machines

Less than 1000 virtual machines

1000 virtual machines or more

29 There is speed variation of simulated networks in the environment

Yes

No

I don't know

30 Number of physical workstations in the environment

Less than 30

Less than 60

Less than 90

90 or more

31 Total number of physical displays connected to workstations during a cyber exercise

Less than 30

Less than 60

Less than 90

90 or more

I don't know

32 Have you done cyber range federation or integration?

Yes

Not yet, but planning

No

I don't know

33 Select the integration / federation technologies you have used or are planning to use

SSH Tunnels

IPSEC Tunnels

MPLS-VPN

VPLS

SD-WAN

Other

34 Our cyber range has dedicated Internet connectivity

Yes

Not yet, but planning

No

35 Internet connectivity speed

Less than 10 Mb/s

10 Mb/s

100 Mb/s

1 Gb/s or higher

36 Latency - Round-Trip-Time (RTT) to Internet

75ms or less

over 75 ms

I don't know

37 Below are my business contact details, which I want to voluntary provide for interview purposes

Yes

No

38 You may send me a notification email when the CS4E project report on cyber ranges is available

Yes

No

39 Contact information

39.1 Name

39.2 Business e-mail

Annex B: Interview questions

1	How would you classify your environment, is it a cyber range, test lab, a test bed or something else? If something else, what is the classification you use?
2	By stating that you have done federation or are planning to do it, can you explain use case(s) or the benefits you are looking after by federating cyber ranges?
3	By stating that you have done federation or are planning to do it, a question about the federation term. Do you find that Federation is sharing scenarios or other operative data related to an exercise in machine readable form being Operational Federation?
4	By stating that you have done federation or are planning to do it, a question about the federation term. Do you find that Federation is technically (at network level) sharing network resources or services therein, being Technical Federation?
5	Do you have requirements to share regarding to federation or can you share a reference URL?
6	Are there certification requirements for the environment you refer, for the facilities in which the environment is operated, or the staff operating or accessing the environment?
7	Can you disclose the requirements or the standard family you are referring in you previous answer?

Optional questions, which will be discussed only if there is time available from the 20 mins appointment time.

8	Are the any technical prerequisites for the participants?
9	Does your environment support hybrid solution, i.e. does it also utilize public cloud services, such as Amazon AWS, Microsoft Azure, Google Cloud, Aliba or some other?
10	Does you environment include possibility to automate red team workflows, i.e. deploy injects/attacks via a tool?
11	Do you have a business model to your trainings or exercises, or operate the environment, which you can explain or open up?

Annex C: Needs (requirements) for IoT security testing and certification

Technical or non-technical requirements for the exercise environment:

- Tools for different techniques of security testing (e.g., Model based testing, penetration, fuzzing, code based testing, etc.).
- Simulation environment of high scale scenarios with support for different IoT devices with different technical characteristics.
- Tools to support modelling and risk assessment (e.g., UML representation, attack graphs).
- Automated testing tools (e.g., TTCN3, JUnit).
- Network tools for packet sniffing and port analysis.
- Simulation of attacks (e.g., DoS, Botnets, brute force).
- Monitoring and Intrusion detection tools.
- Tools for MUD generation (e.g., MUDgee).
- Common cryptographic and protocol libraries available for its usage (e.g., AES, RSA, DTLS, COAP)
- Specific tools for programming IoT devices (e.g., ContikiOS, Cooja)
- Tutorials and manuals of usage for the tools. Even tutorials about common attacks and security best practices.
- Debugging environment.

Requirements for the facilities where the exercise environment is run or used:

- Resilience to support failures.
- Encrypted communications.
- Lifecycle support, including software updates and patches.
- User accounts.

Requirements for the attacks used in the environment:

- Automated execution.
- Complex attacks involving several components and cascade effects.
- Detailed report of the attack result.

the staff operating the environment:

- Good knowledge about the common security testing and assessment tools and the issues that can appear during the exercise.
- Knowledge about IoT implementation environments (e.g., Contiki) and the issues that can appear during the exercise.

Requirements for the staff planning and executing the exercises:

- Good knowledge about the common security testing and assessment tools.
- Good knowledge about the common attacks.