EUROPEAN CYBER SECURITY ORGANISATION

WG5 PAPER

Understanding Cyber Ranges: From Hype to Reality

SWG 5.1 I Cyber Range Environments and Technical Exercises

MARCH 2020

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.
ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg5_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

This document aims to provide an overview of cyber ranges, beginning from their definition, use cases and functionalities while also looking at the different types of technologies and business models that currently differentiate them. The objective of this document is to provide the reader with a better understanding of cyber ranges and with a set of criteria that can be used to better identify and select suitable cyber ranges to meet specific needs and requirements.

2 Acronyms

APT – Advanced Persistent Threat
API – Application Programming Interface
Bins – Binaries or Executables
CDX – Cyber Defence Exercise
CNCI – Comprehensive National Cybersecurity Initiative (US)
CNO – Computer Network Operations
CR – Cyber Range
CRP – Cyber Range Platform
CTF – Capture The Flag
DDOS – Distributed Denial of Service
ICT – Information and Communication technology
IoT – Internet of Things
Libs – Libraries
OS – Operating System
OT – Operational Technology
UI – User Interface
VM – Virtual Machine

3 Definitions

Capture the Flag (CTF) – In the context of computer security, a CTF is a type of cyber war game, which can be played either in teams or as individuals. A popular type of CTF is attack and defence where participants compete to compromise other participants' systems while at the same time trying to defend their own.

Competence – Competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks.

Computer Network Operations (CNO) Units – These are units located within a state's military structure that are tasked to engage in operations involving computer networks.

Cyber Capabilities – Cyber capabilities are the resources and assets available to a state to resist or project influence through cyberspace [1].

Cyber Defence Exercises – Also more commonly referred to as CDX, a cyber defence exercise is a special type of cyber exercise focused on testing cyber defence capabilities.

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.

Cyber Resilience – Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources [2].

Orchestration – Orchestration is the automated configuration, coordination, and management of computer systems and software.

Hypervisor – A hypervisor is the software layer between the hardware and the virtual machines (VMs). It coordinates the VMs ensuring they don't interfere with each other and that each has access to the physical resources it needs to execute.

Platform – A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed [3].

Scenario – A scenario is 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, some practical or theoretical challenges, or different types of questions.

Self-provisioning – Self-provisioning, commonly known as the cloud self-service, is a feature among many cloud service providers which allows their end users to provision resources by themselves and set up or launch a service or application without the intervention of dedicated IT personnel or the service providers themselves [4].

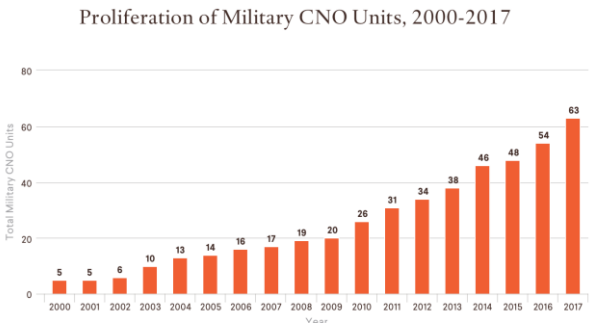
Virtual Machine – A virtual machine (VM) is a software programme simulating the behaviour of a physical computer.

4 Background and Context

The last two years have seen the development of a number of cyber range technologies, products, and national and international initiatives. That is no coincidence and, marketing buzzwords aside, there are several reasons why cyber ranges have suddenly become increasingly popular and more organisations, both private and public, are beginning to invest in them. At a high level, the two key drivers responsible for the growing demand for cyber ranges are the cementing of cyber as a separate domain of warfare and the development and wide spreading of cloud technology, acting as a major enabler for cyber ranges to develop.

4.1 Cyber as a Separate Military Domain

The end of the cold war and the associated race to acquire nuclear capabilities has transitioned into information warfare and the race to acquire cyber capabilities, which can be defined as the resources and assets available to a state to resist or project influence through cyberspace. Nation states are now investing in technologies, methods and processes to develop those cyber capabilities and cyber ranges are being looked at as the equivalent of a traditional firing range where future generations of cyber soldiers will go through cyber-attack and cyber defence simulation exercises. A study by the Council on Foreign Relations shows how the number of Computer Network Operations (CNOs) Units around the world has increased over the last 15 years [1].



In Europe, annual live-fire cyber exercises “Locked Shields” and “Crossed Swords” have been organised in Estonia by the NATO Cooperative Cyber Defence Centre of Excellence and more and more has been invested by governments every year to develop the NATO cyber range. Other examples include the ENISA Cyber Europe exercises which simulate large-scale cybersecurity incidents that escalate to become cyber crises.

4.2 Commoditisation of Cloud Technology

Computer virtualisation and powerful computing resources have reached a high level of commoditisation, allowing to slowly shift the scalability of hands-on education and training to unprecedented levels. Commoditisation of virtualisation and computing technology is also changing the way training and education is conceived and delivered allowing more elaborated forms of continuous learning and continuous professional development, not to mention the way the competence assessment is also positively affected.

5 What is a Cyber Range?

The meaning of cyber ranges has changed over the years and so has the way they have been defined. A review of currently existing definitions and interpretations from around the world from both private and public sector cyber range initiatives broadly identifies two possible ways of defining a cyber range:

A simulation environment – This view of the cyber range focuses on what cyber ranges have traditionally provided, which is a simulation of ICT and/or OT environments to be used for a wide set of purposes. Some definitions look at cyber ranges as inclusive of the Internet services, which are connected to the simulated environment. This way of defining cyber ranges is somewhat static as it usually refers to a simulation environment which is designed once to meet specific use cases and requirements and where any change in the environment requires considerable time and effort.

A platform – A platform is usually defined as a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In the context of cyber ranges, a platform can be intended to be a group of technologies that are used to create and use a simulation environment. The emphasis here is on the word "use" since for a cyber range to be used for specific purposes, the cyber range must have additional capabilities and expose specific functionalities to the end user. This view of the cyber range is clearly more dynamic as it implies that different environments can be more easily created and that functionalities are provided to help in the use of the simulation environment. How easy it is to dynamically create different simulation environments and the breadth of functionalities offered will then vary across different cyber ranges. NIST's definition, for instance, falls into the first interpretation of what a cyber range is, making no reference to services and/or functionalities to be provided by a cyber range other than the simulation environment [5]:

> *"interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer."*

The challenge in defining cyber ranges purely from the point of view of the simulation environments can be compared to the challenge of defining a car in terms of its generic technical characteristic such as having 4 wheels, an engine, a gear box, a seat for the driver and for other passengers etc. The Cambridge dictionary defines a car as:

> *"a road vehicle with an engine, four wheels, and seats for a small number of people"*

When it comes to cars though, men have nearly 200 years of experience and they can easily differentiate between sport cars, F1 cars, SUVs, cabrio, 4x4 etc. and they can, to a varying degree of ease, look for and select the right car based on their specific needs. The same cannot be said for cyber ranges which have only been around for a few years. Just like cars, cyber ranges can be

used for different purposes and by different types of users. However, unlike cars, cyber ranges have evolved to be highly configurable to the point that while we cannot easily convert a F1 car to a family car, we can much more easily use a cyber range for multiple purposes such as security research, security training, assessing cyber resilience and more. The great majority of existing cyber ranges from both the public and private sector do offer additional capabilities beyond the mere simulation environment. Furthermore, most cyber range use cases require one or more capabilities beyond the simulation environment. Therefore, it is logical to infer that a cyber range would be better defined as a platform rather than a simulation environment. On that basis, ECSO defines a 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.*

5.1 Target Users and Use Cases

Cyber ranges can be used for many purposes and the main purpose over the years has changed in line with the changes in technology and the increasing importance of cyber, especially as a dimension of a country's military capability (cyber capability). The use cases described in this section are not presented in order of importance or of highest demand from the market. For each use case, it is important to understand that, in order to fully meet the specific requirements of the use case, a cyber range must possess or expose specific functionalities and/or capabilities. Therefore, this section focuses on what a cyber range can be used for and not on the specific cyber range functionalities, capabilities or even technologies that would be best suited for each use case.

Cyber ranges can be used by a wide range of target users. However, not every cyber range is open or meant to be used by every category of users. The following is a list of target users and target entities of a cyber range:

- Corporates (private and government)
- Strategic decision makers (private and government)
- Security professionals
- Military agencies and CNOs
- Security Operations Centres (SOCs)
- Educators
- Students
- Researchers
- Event organisers

5.1.1 Security Testing

Along with security research, this is the most traditional use case of cyber ranges where system and application simulations are tested and security attacks are carried out against them, in a controlled way, to identify potential vulnerabilities before deployment and use.

5.1.2 Security Research

Cyber ranges are a fundamental means to carry out security research across a wide range of security domains. By their very nature, cyber ranges are themselves being developed by researchers around the world in order to research new attack detection and mitigation methods, malware emulation, and much more.

5.1.3 Competence Building

The majority of security training today is done through online and face to face training courses. In both cases, most of the learning occurs through listening to videos or live lectures, and through reading notes or slides. Relatively little time is spent on hands-on learning. The use of cyber ranges changes that as it can provide a convenient and more cost-effective way of delivering hands-on training, as well as the associated training assessment and certification. According to Gartner, by 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams, up from less than 1% today [8].

5.1.4 Security Education

Security education specifically refers to academia as opposed to the lifelong learning and training that professionals undergo after they leave university. One of the recurring complaints from industry is the lack of hands-on experience by young graduates. The root cause of such a gap is the cost and complexity of providing students with hands-on experience while at the same time not diluting the educational value of university degrees. Universities around the world have begun looking at cyber ranges as a means of improving teaching and learning.

5.1.5 Development of Cyber Capabilities

Cyber capabilities are the resources and assets available to a state to resist or project influence through cyberspace. At a human level, cyber capabilities coincide with the competences of security professionals across a wide range of cyber-attack and defense domains. In such context, cyber ranges are part of a country's cyber capabilities and can be used for developing the capabilities of security professionals, for the research and development of cyber tools and other assets, and for the continuous delivery of cyber exercises to test those cyber capabilities. Specifically, cyber ranges allow a country to carry out cyber capability development at a whole different scale and level of efficiency. Also, within the context of cyber capability development, cyber ranges can be used to organise large scale cyber exercises involving hundreds to thousands of people.

5.1.6 Development of Cyber Resilience

Cyber resilience refers to the capability of an organisation to respond and be able to sustain a security incident or cyber-attack while maintaining its ability to deliver its core business services. NIST defines cyber resilience as *"the ability to anticipate, withstand, recover from, and adapt to*

adverse conditions, stresses, attacks, or compromises on systems that include cyber resources" [6]. Gartner defines it as *"...the degree of adaptiveness and responsiveness to a threat to or failure of digital business ecosystems*" [7]. Overall, cyber resilience applies to any process, system, business and organisation where there is a reliance on IT, OT, IoT which pretty much covers the majority of organisations in a nation, including critical infrastructure. In the context of cyber resilience, cyber exercises provide opportunities for organisations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. Cyber exercises can be divided into 'Capture The Flag' (CTF) and live-fire exercises. CTF are usually organised in attack and defence style where individuals or teams have to find and fix vulnerabilities in their own systems while simultaneously attacking systems that belong to other participants. Live-fire cyber exercises enable teams to train cyber professionals to detect and mitigate large-scale cyber-attacks while being constantly attacked by a "red team" of hackers. Cyber exercises provide the opportunity to test an organisation's capability to handle complex cyber incidents involving several organisations at the same time, thus simulating the interaction with subcontractors, service providers, customers, etc. upon which modern organisations depend. Cyber exercises also enable organisations to find gaps and areas for development in their processes, procedures, and technologies. By addressing the findings from exercises, organisations can greatly enhance their cyber resilience against modern cyber-attacks.

5.1.7 Competence Assessment

Competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks. As the security skills gap increases, organisations need an efficient way of assessing and selecting the right personnel. Using cyber ranges can allow organisations to perform competence assessment beyond the traditional tests, based on multiple choice questions or theoretical simulations. Cyber ranges allow the assessment to be practical and based on the successful completion of practical tasks and/or on the observation of user behaviour and choices made in the execution of practical tasks or assignments.

5.1.8 Recruitment

As cyber ranges are used for competence assessment, it is also to be expected that they will change hiring practices allowing organisations to better identify, validate and hire suitable candidates. This application is highly dependent on the development of the national and international competence frameworks currently being developed around the world.

5.1.9 Digital Dexterity

Digital dexterity, as defined by Gartner, is ***"****the ability and desire to exploit existing and emerging technologies for business outcomes"* [8]. A colourful and simplified, yet effective, way of describing the use case of cyber ranges in relation to digital dexterity is to think of them as a development environment on steroids. Traditional software development methodologies and security best practices recommend the use of different environments such as developing, staging and production. With the ongoing digital transformation and the requirements to support multiple communication and business challenges, organisations are being challenged to project those very same traditional best practices across different channels while at the same time supporting faster development lifecycles. Terms like DevSecOps have become engrained into the fibre of modern organisations and cyber ranges are being looked at to provide organisations with the ability to

improve the organisation's digital dexterity.

5.1.10 National and International Cybersecurity Competitions

More and more countries are organising national cyber security competitions and participating in international ones as a way of discovering new cybersecurity talents and to help fill the security skills gap. Such competitions are typically delivered as CTFs involving a combination of practical challenges. Cyber ranges are changing the way such competitions have been organised allowing for more large-scale events and more realistic simulations. Notable examples include the European Cyber Security Challenge organised by ENISA [9], the Word Skills [10], and the CyberStars competition [11].

6 Cyber Range Functionalities and Capabilities

This section contains a description of functionalities offered by cyber ranges. The emphasis here is on the technical capabilities embedded into the cyber range itself available either to the cyber range end users or its administrators. By definition, a cyber range does not need to include all or any of the capabilities listed in this section. However, depending on the intended use of the cyber range, certain functionalities can be considered desirable or even de facto mandatory. Where those functionalities are not natively supported by a cyber range, systems and applications from third parties would need to be integrated with the cyber range. In such cases, one must carefully evaluate and address the integration and compatibility challenges that would arise. The following figure illustrates the common architectural components and associated functionalities of a cyber range. It's worth noting that many of the cyber range functionalities in the following figure would also require or at least benefit from user management and scenario management functionalities.

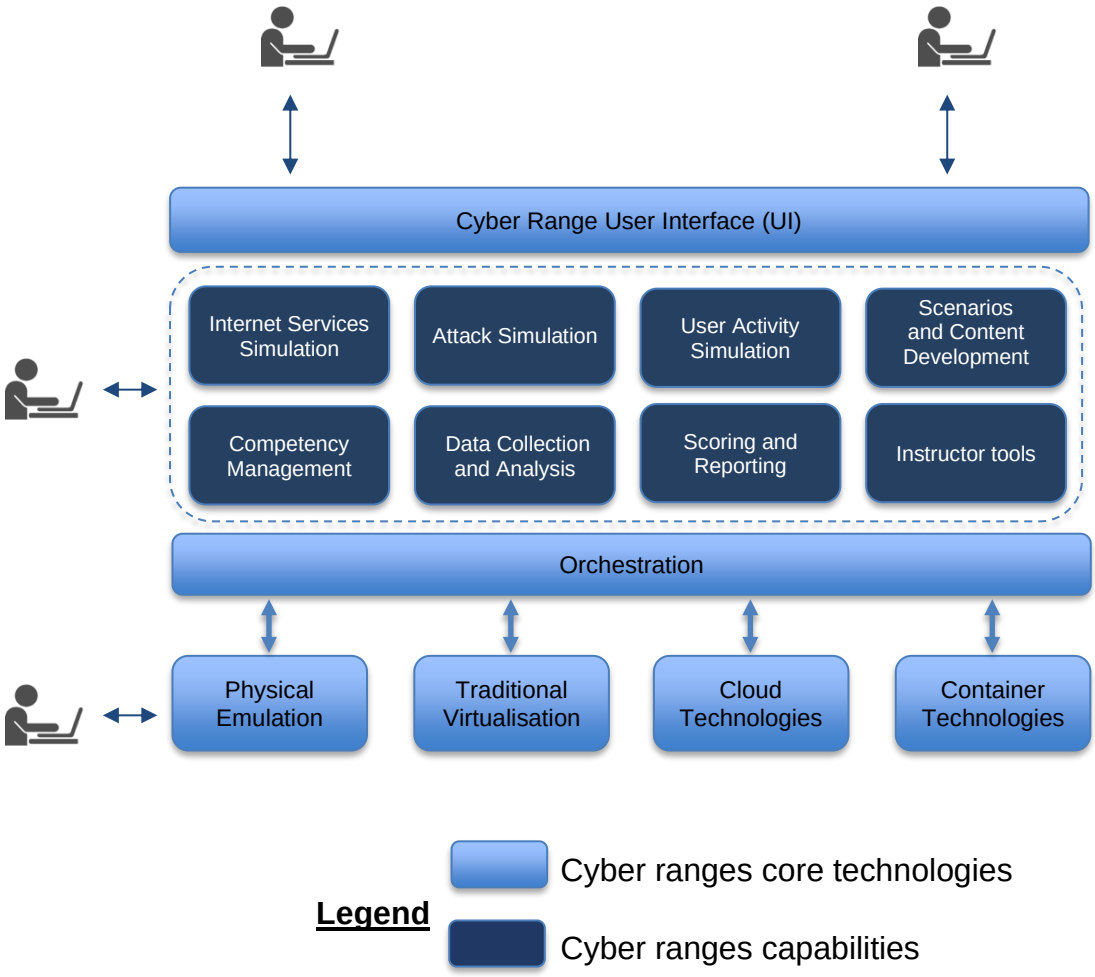


Figure 1 – Sample Architectural Components of a Cyber Range

6.1 Orchestration

Orchestration is the automated configuration, coordination, and management of computer systems and software. In relation to cyber ranges and to virtualisation technologies, orchestration refers to the technology responsible for the creation of automation workflows including the mass configuration, creation, modification and deletion of virtual machines, self-provisioning, and automation of tasks between the virtual infrastructure and other cyber range components or other systems interfacing with the cyber range.

Technically speaking, orchestration falls under the technology section of a cyber range and would be transparent to an end user accessing a cyber range. However, the use of an orchestrator can greatly affect the usability and cost of using a cyber range as well as the support for specific use cases. A cyber range with orchestration capabilities can support additional functionalities, which would otherwise require additional manual effort and coordination and hence additional costs for the cyber range users.

At its most fundamental level, orchestration includes the orchestration of the virtual environment. At its finest, orchestration may also be used to automate tasks and interactions across different components of the cyber range such as the ability to schedule attacks and user simulation, events injection to initiate the collection of user activities and more, depending on the specific use cases.

At a glance, any cyber range scenario involving hundreds to thousands of virtual machines, regardless of the use case, has a de-facto requirement for orchestration.

6.2 Internet Services Simulation

Simulation of Internet services is a broad term to describe any service outside the main simulated environment upon which the simulated environment itself depends for the realisation of a specific use case. Under this category, we find the simulation of social media platforms such as Facebook, LinkedIn, Twitter, app stores, internet routing protocols and different tiers of service providers, controlled update and software repositories for various operating systems, global services such as name resolution, PKI, pgp, public news sites and discussion forums and up to the dark web and TOR network.
Simulation on Internet services adds the realism of scenarios being implemented by the cyber range. Modern attacks utilise global infrastructure and services considerably in order to avoid detection. Therefore, it is very important for cyber ranges nowadays to be able to simulate the Internet and its services realistically. However, in many cases, Internet services are not simulated due to the added complexity required in order to guarantee the right level of realism.

6.3 Attack Simulation

Attack simulation refers to the ability to simulate attacks within and to the cyber range simulated environment. Attack simulation is a growing domain with a number of players and tools [12]. However, the business focus of most attack simulation tools and platforms is the (semi) automatic testing of the corporate security posture. Specifically, attack simulation falls under what is currently known as breach and attack simulation. While traditional vulnerability scanning technology focuses on the identification of systems, networks, and application vulnerabilities, attack simulation tools go the extra mile by allowing to simulate the different phases of the security kill-chain while at the

same time providing recommendations on how to secure the organisation. More recently, breach and attack simulation has been focusing more and more on the MITRE ATT&CK™ knowledge base of adversary tactics and techniques [13], moving away from the traditional security kill chain model. How attacks are simulated is beyond the scope of this paper. However, suffice it to say that the ability to simulate attacks bears a level of complexity comparable to the ability of cyber ranges to simulate ICT/OT environments and that, in fact, one should differentiate between simulation and emulation of attacks. In many cases, attack simulation in cyber ranges is limited to the ability to reply/inject traffic captures with a varying degree of customisation. That is because the breach and attack simulation domain is still developing and is being pushed forward by vendors operating specifically in that domain while it is less common, although highly desirable, amongst cyber range vendors. Desirable features regarding the attack simulation are the availability of an attack library, containing a list of pre-defined attacks, and the ability to import/create custom attacks.

6.4 User Activity Simulation

User simulation refers to the ability to simulate the presence and behaviour of benign users in the cyber range environment. While the technology, tools and methods used may be similar to what is used to simulate attacks, user activity simulation is required for specific scenarios depicting real environments. Besides the actual simulation of systems and applications, user activity simulation is very important as it makes the simulated environment much more realistic. User simulation may refer to both internal users and fictitious client users of the simulated environment. For instance, if the simulated environment is a banking corporate network, user simulation may refer to the simulation of the fictitious banking organisation's members of staff and to the simulation of the clients of the fictitious bank logging in to the online banking website. Examples of user activity simulation include:

- User Internet browsing activity
- Users watching YouTube videos
- Users using P2P file sharing applications to download files
- Users sending emails
- Users interacting with cloud services such as Office 365, Dropbox etc.

User activity simulation also includes the simulation of mobile phones and desktop technologies through which it is possible to simulate user interaction with the target environment. Desirable features regarding the user simulation are the availability of a simulation library, containing a list of pre-defined user simulations, and the ability to import/create custom simulations. Finally, realism is further achieved through the simulation of users and following business processes using the business systems simulated by the cyber range.

6.5 Scenarios and Content Development

The usefulness of a cyber range is ultimately highly correlated to how the cyber range is used, which in turn is correlated to the scenarios the cyber range can be used to deliver. That is somewhat comparable to the experience of using a computer gaming console which is related to the number of available games and the number of third parties developing games for the console. In relation to cyber ranges, the game is represented by the scenario, and the ability to support the development

of scenarios by third parties, or by the users themselves, greatly enhances the usefulness and value added of the cyber range. Some cyber ranges have therefore begun to equip themselves with scenario composition tools, which can include anything from the ability to create basic simulation environments up to full scale custom simulation of attacks and other services.

6.6 Competency Management

A competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks. For a long time, organisations have been using ISO17024 to certify job profiles through the execution of job task analysis which would identify the competences associated to a specific job in relation to the job-specific tasks. More recently, work has been done at national and international level to define competence frameworks which include comprehensive taxonomies of competences and models to define new job profiles or roles. Some frameworks also sample job profiles, demonstrating how the framework can be applied. Notable competence frameworks include the NIST NICE Framework [14] and the European e-Competence Framework (eCF) [15].

Competency (or competence) management systems (CMS) are systems which allow an organisation to manage a competence programme from skills gap analysis and user profiling up to the definition of learning paths and competence assessment. As such, competency management systems may also include a learning management system (LMS) for the administration, documentation, tracking, reporting, and delivery of learning and assessment content.

6.7 Data Collection and Analysis

Data collection refers to the capability of the cyber range to collect users' interaction with the cyber range such as traffic generated, memory dumps, tools used, systems targeted etc. At the most basic level, such capability may just include the collection of data provided by the users (e.g. answers to tasks or challenges). At its most advanced level, it will collect all user interaction. This capability depends on the cyber range's core technologies and how the simulation environment is created since some technologies may provide better native support for the data collection while others would require further development, customisation or integration of third-party solutions.

Data analysis refers to the capability of the cyber range to more easily allow the analysis of the collected data to learn about how the cyber range is used, how users perform etc. In this regard, data analysis of both automatically collected data and of the output of user activities underpins the ability to provide meaningful feedback to the cyber range users. The analysis part may also include AI technology. Given the specialised nature of AI technology, such analysis capability is less likely to be a core cyber range technology and more likely to be a third-party solution integrated within the cyber range.

6.8 Scoring and Reporting

Scoring provides an out of band capability to allow users of a cyber range to be scored based on their activities and interaction with the cyber range. This is the approach followed by many cyber ranges where the focus has traditionally been on the simulation environment itself and not on the management of users and their interaction with the cyber range. Scoring systems can be as simple as collecting user input to questions and tasks, up to more complex attack and defence systems

which include automatic tests for checking service availability, system integrity etc. Scoring systems also include functionalities such as the ability to monitor the progression of user activities and to show a timeline of individual and team performance, while emphasising the different roles in a team. In order to achieve high scoring capabilities, a strong coupling and integration is needed between the cyber range and the scoring system to the extent that some scoring systems have been further developed to include native cyber range capabilities. The reporting side may include a list of standard reports (e.g. per user or per team playing the scenarios) and the ability to create new custom reports that an organisation can use to better visualise its cyber resilience or performance over time etc. It is important to note that most additional cyber range capabilities include and/or require to a lesser or greater extent some reporting capabilities. Finally, while not in the strict sense of the word, reporting also includes real-time cyber situational awareness to allow to clearly visualise the use of the cyber range, the impact of tools used, and action taken by the cyber range users (especially in the context of a cyber exercise).

6.9 Instructor Tools

Instructor tools refer to the capabilities desired and/or required by an instructor using the cyber range for either educational and/or training purposes. Depending on the specific cyber range core technologies, some functionalities such as user session mirroring may not be available, not even through third party components. Furthermore, instructor tools should support the evaluation of users and their action. These data are crucial for providing feedback and evaluating objectives and goals during CDX and CTF. Sample functionalities include:

- Communication facilities (e.g. chat, event broadcasting etc.)
- Instructor mode functionality to show sample answers
- Ability to control the workflow of the scenario (stop, pause, interrupt the execution of the scenario)
- Ability to record and replay users' screen session
- Ability to record and review users' actions (e.g. commands executed)
- Ability to analyse recorded users' actions and other collected data
- Ability to carry out user evaluation
- Ability to deliver user evaluation and feedback, and associated reports

7 Summary of Functionalities vs Use Cases

The following table compares cyber range functionalities to the different use cases. Each cyber range capability is marked as (D) Desirable. It is important to highlight that each cyber range, regardless of the offered functionalities, could potentially be used for a wide range of different use cases. The difference between cyber ranges lies primarily in the amount of work required for each cyber range to deliver specific use cases. For instance, when addressing the cybersecurity training use case, while a native orchestration functionality is desirable, one could equally adopt a cyber range which does not support orchestration, where the orchestration is substituted by manual effort or by adaption of the cyber range usage workflow. Finally, based on the definition provided in this paper and the identified cyber range capabilities, it could be argued that a modern powerful laptop containing a virtualised environment could be considered an extreme example of a cyber range, yet one that is focused on the delivery of training and education activities to a small group of users. Ultimately, the choice of cyber range should be based on the intended use cases.

Functionality	Cyber Range Use Cases									
	Security Testing	Security Research	Competence Building	Security Education	Development of Cyber Capabilities	Development of Cyber Resilience	Competence Assessment	Recruitment	Digital Dexterity	National Cyber Security Competitions
Orchestration			D	D	D	D	D	D	D	D
Internet Services Simulation						D				
Attack Simulation	D	D	D	D	D	D	D			D
User Activity Simulation		D			D	D				
Competency Management			D	D	D	D	D	D		D
Scenarios and Content Development			D	D	D	D	D	D		D
Data Collection and Analysis		D	D	D	D	D		D		D
Scoring and Reporting			D	D	D	D	D	D		D
Instructor Tools			D	D	D	D	D			

Table 1 - Cyber Range Functionalities vs Use Cases

8 Cyber Range Technologies

When talking about cyber range technologies, the focus of the discussion shifts to virtualisation since it is the only technology that allows the creation of cost effective and efficient simulation. Naturally, not everything can be simulated by using virtualisation technologies and some parts of a simulation environment may indeed require physical components. However, most use cases of a cyber range can be achieved through virtualisation. With that in mind, cyber ranges can be broadly divided into two types, based on the main technologies used to develop them:

1) Conventional Cyber Ranges – These are cyber ranges based on conventional virtualisation
2) Cloud-Based Cyber Ranges – These are cyber ranges based on cloud technology

As cloud technologies and conventional virtualisation continue to evolve, a third type of hybrid cyber ranges will also begin to develop, based on the use of the different technologies. Such type is not covered in this paper.

8.1 Conventional Virtualisation

The following figure illustrates the basic types of conventional virtualisation, including traditional hypervisor-based virtualisation and container technology. Many cyber ranges rely on one or the other, or a combination of the two.

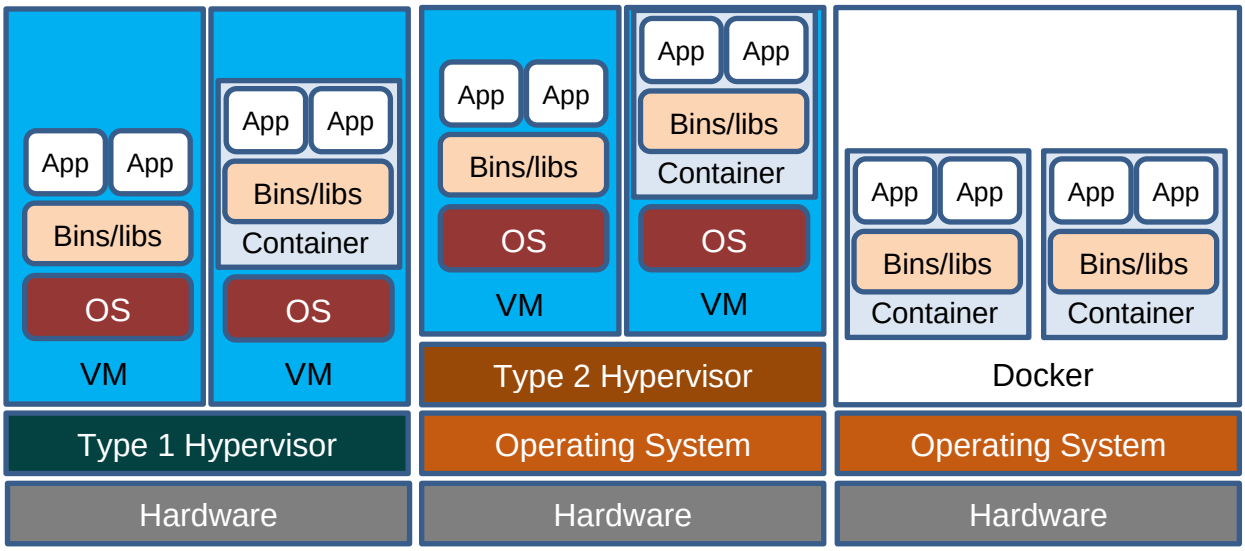


Figure 2 - Conventional Virtualisation

It is worth noting that in the above figure, the container technology is represented by Docker whereas no specific examples are illustrated with regards to traditional virtualisation. This is because, unlike the traditional virtualisation characterised by many technological flavours, the container technology is de facto dominated by the Docker technology.

8.1.1 Traditional Virtualisation

Traditionally, virtualisation is achieved through the creation of a virtual machine which is a software

programme simulating the behaviour of a physical computer. Since multiple virtual machines can run on real hardware, an extra software layer is used, called hypervisor, which ensures that virtual machines do not interfere with each other and that each has access to the physical resources it needs to execute. There are two types of hypervisors [16]:

- Type 1 or “bare-metal” hypervisors interact with the underlying physical resources, replacing the traditional operating system altogether. They most commonly appear in virtual server scenarios and therefore for the development of data centres.
- Type 2 hypervisors run as an application on an existing operating system (OS). They are most commonly used on endpoint devices to run alternative operating systems and carry a performance overhead because they must use the host OS to access and coordinate the underlying hardware resources.

Sample hypervisors are listed in the following table.

	Type 1	Type 2
Commercial	• VMware's ESXi (data center-focused) • Microsoft Hyper-V • XenServer, now known as Citrix Hypervisor • IBM z/VM	• VMware Workstation (Player or pro) • Parallels
Opensource	• KVM (kernel-based virtual machine)	• VirtualBox • QEMU

Table 2 - Sample Hypervisors

Several cyber ranges exist which have been built on traditional virtualisation, especially those cyber ranges that were built before the widespread of cloud technology. The majority of such cyber ranges have been built upon commercial virtualisation providers (for the most part VMware) which accounts for large investment costs and large running costs associated to the annual licensing of the virtualisation software. By its very nature, traditional virtualisation does not have an advanced level of orchestration so the cyber range provider would need to develop on top of it. Also, traditional virtualisation technology has been developed with data centres in mind, to provide organisations with the ability to manage hundreds of servers much more efficiently and cost effectively. However, the main use case for traditional virtualisation is to have servers running (boot once and reboot when needed) and not to have a large number of both servers and clients dynamically boot, shut down, delete, configure on demand etc. For this reason, cyber ranges built on traditional virtualisation are not characterised by a strong level of orchestration. However, unlike cyber ranges based on public clouds, cyber ranges built on traditional virtualisation benefit from a great level of flexibility and control which, based on the development work done by the cyber range provider, can include support for different capabilities and most importantly the control over the cyber range data and information.

8.1.2 Container Technology

The other traditional approach to virtualisation, one which has witnessed huge technology developments in recent years, is the one based on containerisation technology. Unlike conventional virtualisation where each virtual machine runs its own operating system (OS), containers share a

machine's operating system kernel. Specifically, container technology has been developed to facilitate and improve portability of applications across different computing environments by bundling the application code together with the related configuration files, libraries, and dependencies required for it to run.

Container technology offers cyber range vendors the ability to run multiple containers on the same virtual machine. Container technologies also provide orchestration capabilities able to pre-configure complex networks and inter-container communications making them more cost-effective. However, because of their very nature, container technologies do not simulate a real system but rather a stripped-down version of an environment designed for the sole purpose of running an application. The scope of simulation offered by containers is therefore limited. For instance, while container technologies have been working on Windows systems for quite some time now, they are somewhat limited in the ability to simulate a full Windows system. Specifically, you cannot simulate a full Windows infrastructure with Active Directory, Windows servers, and Windows workstation, using only containers. For this reason, the most common use cases of cyber ranges based on container technology are related to security training and education, but not all types of training can be addressed. When it comes to security, both container and virtualisation technologies have inherent issues. When using containers, all individual applications run under the same host and are isolated, at software level, by the operating system. Misconfigurations of individual containers or vulnerabilities affecting the host kernel can lead to sensitive data exposure or even compromise of adjacent containers. Such attacks can be mitigated by enforcing strict configuration and patch policies on individual container hosts. One of the advantages of container technology is that security patches can be easily deployed with minimal disruption. On the other side, traditional virtualisation technologies function at the hardware level. Misconfigurations of the hypervisor are a possibility, but a very slim one. Vulnerabilities still exist on the hardware or hypervisor level which would allow attackers to compromise the host and any adjacent virtual machines running on it. Although the frequency of such vulnerabilities being published is low, that doesn't necessarily mean they do not exist. Mitigation can be achieved with minimal interruption, since virtualisation technologies usually allow for host migration, and by enforcing strict patch policies and procedures.

Gartner predicts that by 2022, more than 75% of global organisations will be running containerised applications in production, compared to fewer than 30% today [17]. In the coming years, it is safe to assume that cyber ranges will be requiring an increasing capability of simulating containers.

8.2 Cloud Virtualisation

With conventional virtualisation, resources are not efficiently used and in fact it is not natively possible to tap into unused physical resources that span across an entire infrastructure. While building on conventional virtualisation, cloud virtualisation abstracts the underlying physical resources across an entire infrastructure (ram, disk space, network etc.) and makes them available transparently to the hypervisor to be able to better and more fully utilise all available resources. As a result, the most immediate advantage of cloud virtualisation is cost reductions by increased efficiency. However, another great advantage that comes with cloud virtualisation is its native orchestration capability to automate and facilitate the workflow management of virtual machines. It is important to note that cloud technologies make available to users both traditional hypervisor-based virtualisation and container technology virtualisation. In other words, it is possible to run both standard virtual machines and containers on the cloud, depending on the specific cloud technology and vendor.

The inherent support for dynamic configurations, increased efficiency and scalability makes cloud technology a natural choice of implementation for modern cyber ranges, although not for all cyber range use cases and not necessarily across the different types of cyber range users. Specifically, three types of cloud-based cyber ranges exist which are related to the same three types of cloud deployments normally used for standard business applications.

8.2.1 Public Cloud

In a public cloud environment, the cloud services are open to the public for subscription, which allows users to access services without having to worry about running or maintaining the cloud infrastructure, which is done by the cloud provider. Public clouds are mostly run on a pay-as-you-go model, which allows the development of cyber ranges to start off without heavy initial investments and hardware procurement headaches. Usually, public cloud providers give access to their cloud virtualisation through APIs and all that a cyber range provider must do is develop the cyber range platform on top of it, leaving all the heavy lifting to the cloud provider. That is probably the reason why many of the cyber ranges which have appeared on the market recently are based on public cloud providers. Examples of public cloud providers include Amazon Web Services (AWS) , Microsoft Azure, Google and Rackspace.

While easier to set up and operate, public cloud-based cyber ranges do offer several drawbacks which one must take into consideration. The first one is the inherent lack of control over the data that flows through the cyber range. Another main disadvantage is the lower level of flexibility required by the cyber range vendor in order to develop and configure bespoke scenarios and to offer some of the cyber range capabilities outlined in this paper. Every new cyber range capability, beyond the core one of creating and managing simulation environments, must face the technology constraints of the cloud provider. For this reason, the majority of available public cloud cyber ranges are mostly focused on the training and education use cases where the ability to quickly and efficiently manage the workflow of simulation environments comes as a great advantage. Other drawbacks of public cloud-based cyber ranges are related to the limitations imposed by the public cloud provider to deliver simulated attack scenarios including but not limited to DDOS attacks or any other disruptive-type of attacks which may affect the public cloud infrastructure. Finally, while the pay per use model may be advantageous, public clouds are notorious for charging users based on different factors such as disk space, Internet bandwidth etc., which can quickly get out of hand if not managed correctly.

8.2.2 Private Cloud

Private Clouds are created and maintained by a private organisation for its own private use or to offer services to its clients. To build a private cloud, an organisation must bear all the cost of setting up, maintaining and operating the cloud infrastructure. The flipside benefit of running a private cloud is the total control over the applications, data and information flow within the cloud infrastructure. For this reason, private cloud cyber ranges, along with cyber ranges based on conventional technology, may be a more suitable choice where privacy and confidentiality are mandatory requirements, such as for government or military applications. Like cyber ranges based on conventional technology, private cloud cyber ranges also have great flexibility in the development of additional cyber range capabilities, beyond the core ones, either natively through the vendor's own development work or through the integration of third-party systems and applications. The combination of these factors also gives cyber range vendors based on private clouds the ability to offer on premise options for the cyber range, which public cloud cyber ranges cannot do.

Just like conventional cyber ranges, private cloud cyber ranges are well suited to provide support across the wide set of cyber range use cases, with the added benefit of making use of cloud technology orchestration. Cyber ranges built on private clouds can be built on both commercial and open source solutions. Vendors based on commercial cloud technology are likely to carry a higher price tag associated to the licensing of the technology upon which they depend, but they also enjoy stronger technology support from the cloud provider network. The most common open source technologies used for building private clouds include Openstack and OpenNebula.

8.2.3 Hybrid Cloud

Hybrid clouds, just as the name implies, combine the best of both worlds. A hybrid cloud is an infrastructure that includes links between the private cloud, managed by the organisation, and at least one public cloud, managed by a third party (e.g. Amazon, Microsoft etc.). Hybrid clouds offer stronger controls, especially with regards to the security of critical data, assets, and operations while at the same time leveraging the natural scalability of the public cloud infrastructure. Cyber ranges built on hybrid cloud technology can apply better control to the sensitive data associated to the range. While cloud providers go to great lengths to protect their customers' data, public clouds are fundamentally much more open environments than a private network, which makes them more vulnerable to cyberattacks and various forms of data leakage. The use of cyber ranges generates data which can provide an insight into the cyber capabilities of an organisation or a country. This is a major consideration especially when using cyber ranges developed on public clouds. Therefore, some organisations, especially privacy sensitive ones from the military and government domain, can benefit from the advantages of cyber ranges built on hybrid cloud technology. Ultimately, great care needs to be put into deciding what services are run on the public infrastructure and what information must remain on premises.

9 Inter-Cyber Range Communication

Initiatives are being brought forward which bring together multiple cyber ranges in a way to increase or improve simulation capabilities as well as other capabilities beyond what can be offered by a single cyber range.

9.1 Federation of Cyber Ranges

In information technology, a federation is a group of computing or network providers agreeing upon standards of operation in a collective fashion. 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. The concept of federation is based on the assumption that it is highly complex and costly for a specific cyber range to be able to provide all the required capabilities and functionalities and it is therefore conceivable that multiple cyber ranges, each with its area of specialisation, could work together to offer end users the ability to achieve multiple use cases and different types of scenarios. A federation of cyber ranges can offer users a one-stop shop for all their needs and requirements.

It is important to note here that federation 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. Cyber ranges in a federation may well be able to communicate. However, integration is not a requirement for federation to exist. There are notable examples of cyber range federations being developed in Europe by the European Defence Agency (EDA) [18], and the EU-funded project ECHO [19]. The CyberSec4Europe [20] project will demonstrate requirements, specifications and use cases for federation of cyber ranges during 2020 and 2021.

9.2 Integration of Cyber Ranges

Compared to the concept of federation, integration does require cyber ranges to talk to one another. Cyber range integration means a group of two or more cyber ranges which can communicate with one another to deliver a simulation environment spread across the cyber ranges. 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. In other words, integration requires discipline in planning the technical network environment. Integration of cyber ranges carries more technical and logistical challenges than a federation of cyber ranges. The technical challenges are related to the ability to orchestrate cyber ranges running on potentially different technologies, along with issues of IP addressing, Internet bandwidth and more. Also, scenario design must take into consideration the different cyber range technologies and potential dependencies. In other words, the benefits of using an integration of cyber ranges is heavily dependent on the scenario being designed and developed to take advantage of those benefits.

10 Cyber Range Delivery Models

Having defined what a cyber range is, the question is “how can one have access to one”? Cyber ranges can be broadly accessed in one of two possible ways, which are:

1) Cyber Range as a Service
2) On-Premise Cyber Range

How a cyber range can be accessed is irrespective of the technology used for the implementation of the cyber range. For instance, while many people may naturally associate the Cyber Range as a Service delivery mode to the use cloud technology (after all, SaaS as a delivery mode is a cloud technology concept), there also exists cyber ranges which are accessible as a service but are not developed using cloud technology or available online.

As cyber range technologies mature, mixed-mode cyber ranges will become more mainstream and begin to appear on the market, providing some of the functionalities on premise within the organisation while leaving other functionalities available as a service (mostly online but also from a physical site of the cyber range provider).

10.1 Cyber Range as a Service

In this model, the cyber range is owned and managed by a cyber range provider who makes it available to third parties with charging models based on the cyber range provider, the specific functionalities and capabilities and, ultimately, the services offered. Two main types of cyber range as a service exist:

- Online – In this case, the cyber range is accessed remotely by the client and is most likely developed on cloud technology, although not necessarily.
- Physical – In this case, the cyber range is hosted at a physical location that the client needs to visit in order to use it. The cyber range will usually provide physical training facilities, break out rooms, and debriefing rooms, which constitute part of the service offering.

As mentioned earlier, the types of underlying cyber range technology can vary, with earlier cyber ranges being developed with traditional virtualisation technology and more recent ones using cloud technology.

10.2 On-Premise Cyber Range

An on-premise cyber range is physically deployed on-premise at an organisation. This is usually the most expensive cyber range option as it requires a larger upfront capital investment associated to the cyber range hardware and software. The on-premise option, while definitely more expensive, is better suited to meet the security requirements of an organisation which can better exercise control over the data associated to the use of the cyber range. As virtualisation technology evolves and broadens the realm of simulation, the cost of on-premise cyber ranges will decrease. By definition, on-premise cyber ranges cannot be built on public clouds and can only be based on conventional virtualisation or private cloud technology.

11 Conclusions

This paper has presented an overview of cyber ranges and associated use cases, emphasising the different capabilities which a cyber range can expose and the different types of technology underpinning the development of a cyber range. Specifically, this paper has introduced a range of criteria which can be used by the reader to better evaluate the capabilities of different cyber ranges as they pertain to the ability to meet the requirements of specific use cases. Finally, this paper has outlined the different technologies underpinning the development of a cyber range, emphasising the intrinsic limitations and/or potential capability of each technology.

It is the authors' opinion that cyber range technologies and cyber ranges today are already very mature to be able to deliver several use cases, yet immature to deliver some of the market expectations and the ultimate promises that cyber ranges aim to fulfil. As the market currently lacks a clear understanding of cyber ranges and the associated technologies and use cases, cyber ranges are chosen indistinctively with the aim to meet specific use cases only for the realisation that not all cyber ranges are the same, thus resulting in failed expectations. As is often the case when a new emerging and trendy technology starts to become widespread in the market, users make hasty decisions which result in the inability to achieve the intended return on investment. It is the hope of the authors that a reader intending to acquire, choose, or develop a cyber range will find the information in this paper a useful guide.

References

[1] Council on Foreign Relations (2018), Understanding the Proliferation of Cyber Capabilities [online], https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities
[2] NIST (2018), Developing Cyber Resilient Systems: A Systems Security Engineering Approach [online] https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft
[3] Techopedia, Platform definition, https://www.techopedia.com/definition/3411/platform
[4] Techopedia, Self-provisioning definition, https://www.techopedia.com/definition/29433/self-provisioning
[5] NIST (2018), Cyber Ranges, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf
[6] NIST (2019), Developing Cyber Resilient Systems: A Systems Security Engineering Approach, https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft-fpd.pdf
[7] Gartner (2018), Organizational Resilience Is More Than Just the Latest Trend, https://www.gartner.com/en/documents/3875514/organizational-resilience-is-more-than-just-the-latest-t
[8] Gartner (2020), Digital Dexterity, At Gartner Digital Workplace Summit, https://www.gartner.com/en/conferences/na/digital-workplace-us/featured-topics/digital-dexterity
[9] ENISA (2020), European Cyber Security Challenge, https://europeancybersecuritychallenge.eu
[10] WorldSkills (2019), https://worldskills.org
[11] Cyber Stars (2019), https://www.cyberstars.pro
[12] Geekflare (2018), 8 Cyber Attack Simulation Tools to Improve Security, https://geekflare.com/cyberattack-simulation-tools/
[13] MITRE ATT&CK, https://attack.mitre.org
[14] NIST, NICE CYBERSECURITY WORKFORCE FRAMEWORK RESOURCE CENTER, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center
[15] European e-Competence Framework, A common European framework for ICT Professionals in all industry sectors, https://www.ecompetences.eu/
[16] IBM (2019), Virtualization, https://www.ibm.com/cloud/learn/virtualization-a-complete-guide
[17] Gartner (2019), 6 Best Practices for Creating a Container Platform Strategy, https://www.gartner.com/smarterwithgartner/6-best-practices-for-creating-a-container-platform-strategy/
[18] European Defence Agency (2018), Cyber Ranges Federation Project reaches new milestone, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone
[19] ECHO Project, https://www.echonetwork.eu
[20] CyberSec4Europe Project, https://cybersec4europe.eu/

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU