Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

D2.1: State of the art cyber range technologies analysis

Document Identification

Status	Submitted
Version	1.0
Related WP	WP2
Related Deliverable(s)	State of the art cyber range technologies analysis
Lead Participant	NAVAL GROUP
Contributors	UoP, ATOS, VTT, ICCS
Due Date	Friday, 31th January 2020
Submission Date	06/05/2020
Document Reference	D2.1
Dissemination Level	Public
Document Type:	Report
Lead Author	MARC LAMOTTE
Reviewers 1	Eleftherios Ouzounoglou Evangelos Sdongos George Baroutas
Reviewers 2	Mathieu Leturcq

Legal Disclaimer

The document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Information

List of Contributors	
Name Surname	Beneficiary short name
THIERRY MAUR, SOUNITA SANDANAKRICHENANE	NG
KIMBERLY TAM	UoP
JUKKA JULKU, SAMI NOPONEN, JARKKO KUUSIJARVI	VTT
GUSTAVO GONZALEZ-GRANADILLO	ATOS Spain
MATHIEU LETURCQ	DIATEAM
MARKOS ANTONOPOULOS	ICCS

Document History

Version	Date	Change editors	Changes
0.1	02/12/2019	NAVAL GROUP	Initial version to be submitted
0.2	20/12/2019	NAVAL GROUP	First range of remarks and version to be submitted
0.3	13/01/2020	NAVAL GROUP	Second range of remarks and version to be submitted
0.4	23/01/2020	DIATEAM	Reviewed Document Report
0.5	28/02/2020	ICCS	Review consolidated report
0.6	12/03/2020	NAVAL GROUP	Updated based on final comments from ELEFTHERIOS OUZOUNOGLOU, GEORGE BAROUTAS and EVANGELOS SDONGOS (ICCS)
0.7	24/03/2020	ICCS	Review and acceptance of the updated deliverable from reviewers
1.0	30/04/2020	ICCS	Final version reviewed by PC

Quality Control

Role	Who (Partner short name)	Approval Date
Deliverable leader	NG	12/03/2020
Quality manager	UoP	30/03/2020
Project Coordinator	ICCS	30/04/2020

Table of Contents

List of Tables

List of Figures

Executive Summary

The Cyber Ranges (CRs) are virtual simulation environments for networks with the capability to incorporate elements like simulated devices, simulated traffics, and others. The purpose is to gain hands-on cyber-skills for the stakeholders without disrupting the production environment.

Apart from increasing the cyber-awareness level of the maritime logistics actors, the challenge for Cyber-MAR is to be able to estimate the financial cost of a cybersecurity risk. Hence, Cyber-MAR can offer functionalities as a decision support tool towards different roles and levels of personnel within various entities.

It is imperative that the platform can play realistic scenarios closer to the real life. Choices of architecture are therefore to be made: emulation or simulation of such a component? Operational technologies hybrid (real/virtual) coupling? Such choices need to be considered not only from a technological point of view but also from a financial perspective so as to ensure the feasibility of such a cybersecurity investment.

An evaluation platform and system of the Cyber Range is mandatory in order to guarantee reliability of the simulation results in return. There is in particular an issue on mastering the interconnection of the various components, and associated test strategy on the component alone, but also its implementation at platform level with its interactions and interdependencies.

This document "D2.1 State of the art Cyber-range technologies analysis" provides points of attention which will be taken into account for the implementation of Cyber-MAR: relevant technologies to the maritime sector and specific to interconnection with SCADA systems. Combined with Cyber-MAR surveys of end-users, this document is also positioned as a structuring document for the Cyber-MAR potential architecture choices.

1. Introduction

1.1 Purpose of the document

The purpose of determining the state-of-the-art facilities and tools related to cyber ranges (CRs) is to help the Cyber-MAR project deliver a unique and novel, cyber-range environment.

By understanding the start-of-the-art for CRs the project will be in a good position for deploying a novel cyber range while meeting the required advanced capabilities for:

- Hybrid simulation
- Intrusion detection/prevention (IDS/IPS)
- Interconnection and interoperability between several CRs
- Data fusion & analytics, situational awareness, scoring system for trainees

Therefore, the purpose of this document is to examine what cyber-range solutions and tools exist today, both generally but also more specifically in the maritime sector or relating to cyber-security topics (e.g., IDS/IPS) so that we may best meet this goal. Additionally, the current research trends in the cyber range domain are visited in order for the design of the proposed solution to be influenced also by the most updated activities in the field.

The writing of this document is carried out in the task 2.1 of the Cyber-MAR project. It is an input document for task:

- T2.2: User requirements related to efficiency, performance, trust, privacy and security
- T2.3: Cyber-MAR System Requirements and Functional Specifications
- T2.4 : Cyber-MAR System Design and Integration Plan

1.2 Intended readership

This deliverable is a public deliverable. While this may increase awareness in targeted maritime domain about CRs the aim is to define the current capabilities and uses of CRs, and how Cyber-MAR intends to continue the evolution of cyber ranges. Therefore, the parties mostly likely to be interested in this document's observations would likely be other organizations working with CRs, i.e. industry, government, academia, and those in maritime or cyber-security.

1.3 Document structure

The methodology followed for composing this deliverable was to visit the related to the field of CRs literature and online material in order to firstly give to the reader a definition on what is a CR, then to identify and describe all the generic components of CR's eco-system and finally, provide a list all tools used in CRs as well as an overview of CR market.

The next sections of the document are structured as follows:

Section 2 is the main part of this document including the state-of-the-art look on CRs in 3 parts:

- The first part is dedicated to provide a definition on what a CR is, including a definition of its setup and its uses/purposes
- The second part, is dedicated to present technologies used in CRs
- The last and third part is dedicated to show a panorama of CRs in academic/ research domain and in the market. This chapter also highlights several state-of-the-art CR concepts and designs across industry, academia, and parts of government.

Section 3 deals with various trends, in particularly on the subjects of cyber-threat, situational awareness, and the changing cyber landscape by presenting the beyond the state of the art findings.

Finally, in Section 4, the conclusions of the deliverable are provided.

1.4 Reference documents

The following documents contain requirements applicable to the generation of this document :

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement – 833389 Cyber-MAR		1	04/17/2019

Table 1 Applicable documents

1.5 List of Acronyms

Abbreviation / acronym	Description
BGP	Border Gateway Protocol
CR(s)	Cyber Range(s)
CSIRT	Computer Security Incident Response Team
Cyber-MAR	**Cyber** preparedness actions for a holistic approach and awareness raising in the **MAR**itime logistics supply chain
DGA	Direction Générale des Armées (French military organisation, General direction of army)
Dx.y	Cyber-MAR: WPx Deliverable number y
EC	European Commission
ECSO	European Cyber Security Organization
EDA	European DefenceDefence Agency
ICS	Industrial Control System
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IoT	Internet-of-Things
IT	Information Technology
NMAP	Network Mapper
OSI	Open Systems Interconnection
OSPF	Open Shiortest Path First
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SSH	Secure Shell protocol
WP	Work Package

2. State of Art

2.1 Cyber range definition

2.1.1 Introduction

Despite the ever-growing adoption of networked technology in almost all areas of contemporary infrastructures, both a standardized technology plus a systematic methodology for testing and evaluation of such systems and related products from a cyber security perspective remain elusive. Pertinent traditional testing assumed that the behavior of such networked systems is determined by the behavior of its individual components; Therefore, traditional testing focused separately on each isolated component by emulating a static interface to the rest of the network. However, the behavior of a networked system, especially in large scales, is dynamic and unpredictable, due to the interaction of its components with external devices. Furthermore, the behavior of such systems is not determined solely of the behavior of its individual components, but also by their highly complex interdependencies.

Apart from testing, the security of contemporary networked infrastructure requires trained professionals and specialized tools, able to detect network vulnerabilities and to respond real-time to cyber threats, analyze them, plus monitor and maintain the network's integrity and secure function. Due to the ever-changing landscape of cyber threats, it is perceivable that cyber-security professionals require continuous, ever-lasting training as cyber security tools require continuous evaluation and updates.

CRs is an emerging technology promising to provide solutions to the above questions. The National Institute of Standards and Technology defines CRs as interactive and/or simulated representations of events of an organization's local network, system, tools and applications [1]. Further to this definition, ECSO WG5 recent publication on CRs [2] provides the following CR definition:

"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."

The evolving cyber threat landscape, leads to the imperative need for the maritime industry to strengthen its cyber resilience. Cybersecurity has vaulted to the forefront as a major challenge for the maritime industry.

In the area of IT security, organizations are faced with the persistence of cyber-attacks, combined with the rise of new threats. At the same time, they are not sufficiently prepared to anticipate incidents and to provide adequate responses.

Staff training remains the primary challenge, resulting in significant investments by organizations. For this challenge, the CRs, computer simulation environments, dedicated not only to the experimentation of technologies, but also to hands on training of the personnel, provide a pertinent answer to this challenge. A key element to whether a CR is useful or cutting edge is its capabilities; how accurately the CR can represent real-world scenarios and problems. As discussed in the following sections, part of what makes the proposed Cyber-MAR CRs cutting edge is the real-world simulation, and emulation, of maritime systems in real-world contexts (e.g., logistics, supply chain).

It should be mentioned that the following review is limited to information that is available in the public domain.

2.1.2 Cyber range Role

As mentioned in the previous paragprah, a CR can be understood as a virtual simulation environment for networks, able to incorporate elements like actual or simulated devices, virtual machines, software, webpages, simulated traffic etc. Security professionals to obtain hands-on skills and insights pertaining to system design and real-time defence against cyber-attacks can utilize this environment. The ultimate objective of these systems is to simulate/emulate real world attack scenarios in complex, large-scale scenarios. More specifically, an ideal cyber range should [1], [3]–[5]:

1. Provide a configurable environment, enabling fast customization to address different network topologies and/or functions (i.e. communications, SCADA etc).
2. Emulate or simulate with high fidelity and performance the actual network infrastructure under consideration.
3. Provide a featured environment where teams and/or individuals may engage in an exercise.
4. Perform data collection throughout the exercise.
5. Provide performance metrics and assessment for the engaged teams.

The configuration of a cyber range into a customized testbed is a non trivial task and poses a number of questions regarding the accuracy of representation and the reliability of the results, with regards to the training of professionals or the testing a cybersecurity product. In the past, such configurations were manual, time-lengthy and error prone. Equally important, they were unable to keep up with evolving training and testing requirements. Through technological advances like the federated CRs described in subsequent parts of the present report, the situation has improved significantly.

However, there are many cases of specialized and/or large scale networks for which current CR technologies does not allow to comply with the aforementioned requirements. Depending on the specialization of the considered network, there are still cases where many components of the cyber range need to be developed nearly from scratch to represent them reliably. Industrial and military networks consist two concrete classes of such examples.

Both contemporary networks plus their potential cyber range representations are highly complex systems. Thousands of interactions, parameters and individual component functions determine their behavior. Exhaustive consideration of all possible hypotheses and scenarios is infeasible. Therefore, the need for strategies indicating where to focus and why remains imperative. Furthermore, as will be detailed below, the trade-off between the required fidelity of the representation and overall cost remains largely open for most real world systems. It is therefore definitely a challenge to define systematic methodologies outlining optimal network representations plus reliable testing scenarios and effective training procedures towards a specified objective. The absence of such methodologies has frequently led to questionable results [4].

The simulation used in CRs provides the opportunity to develop skills in a secure and controlled environment, in which scenarios can be customized to reflect the attacks that teams have experienced or fear to face in the future. In addition, they can be random attacks, or reflect the ever-changing nature of current threats.

More recently, CRs are including not only traditional IT (information technology) systems but are starting to include also cyber physical systems based on Operational Technology (OT), which will be explained further in the following subsections.

2.1.3 Cyber range Classification

CRs are a relatively new and still evolving technology. They can currently be classified to various categorizations, in view of which current research trends on the subject are formulated [3].

By utilization: i.e. product testing and evaluation and/or research and development, and operational training.

Probably the most important CRs categorization is by type [3]–[6]:

a) Simulation type, which utilizes models of each network component to simulate network function. (cost effective, lower fidelity)
b) Ad hoc or overlay type, which utilizes a software overlay on top of the actual components of the network under consideration to add functionality and run tests on them.

c) Emulation type, where the topology of the network under consideration is mapped to the physical infrastructure of the CR. (more expensive, high fidelity)

CRs may also be classified by their supporting sector, i.e. academic, military or commercial.

Many aspects of the current research on CRs takes place in each of the above categories plus their various intersections.
A CR can be composed of different branches related to scenarios, scores, teams, monitors, and management. According to the needs of a CR, it specializes in one or more branches (as shown in Figure 1 **Error! Reference source not found.**):

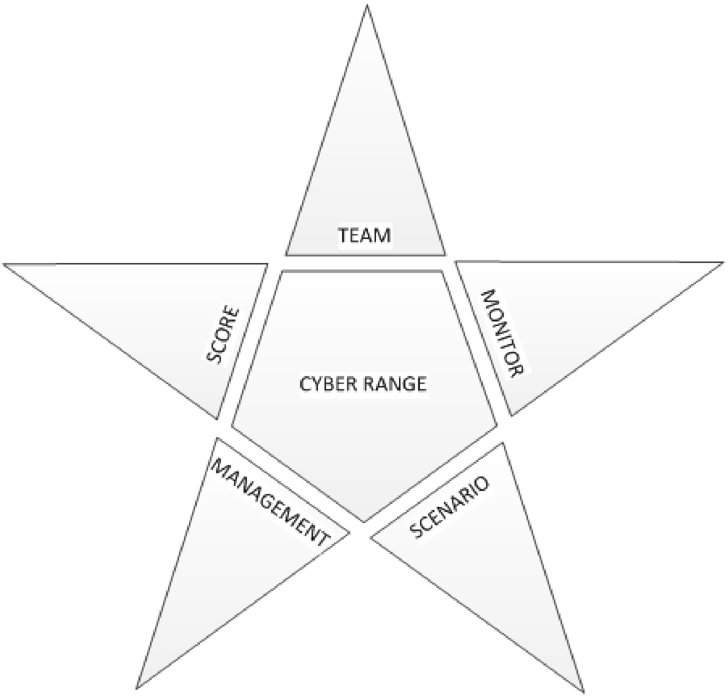

Figure 1 - CR classification

The scenario gives a sense to the exercise training, with a story, a purpose, and an environment in a technical domain.

The score permits to define various indicators in order to measure technical and team performances through methods and tools.

The monitoring is done in real-time during the cybersecurity exercise and tests. It can be realized by human observers or automatically by the use of tools.

The teams are one or several groups of persons with a color associated to a role (See Section 2.1.4).

The management takes care of all the management of the CR from assignment of role, computation allocation, etc.

All CRs can be classified based on these branches as detailed in research [7]. Particularly:

By scenario purpose In the research work "Cyber ranges and security testbeds: Scenarios, functions, tools and Architecture", in [7] it is shown that the number of CRs used for education are rapidly growing from only 3 CRs in 2005 to 7 CRs in 2017. Additionally, and besides training, an important objective is testing. For that purpose, system's security assessment and new defence or attack methods or techniques are closely related. In the relevant literature the same behavior for testing use is noticed from 2002 with 1 CRs to 8 CRs in 2015 (information about 2018 and 2019 are not yet complete).

By Domain scenario: In reference [7] it is additionally shown that:

- The usage of SCADA scenarios start to appear in 2008 and reaches its peak in 2017
- The usage of IOT scenarios appears in 2016.

2.1.4 Generic description of a Cyber range

Humans and technical equipment are the two main sources of stimuli we can distinguish in a CR.

In Figure 2 this categorization is illustrated.

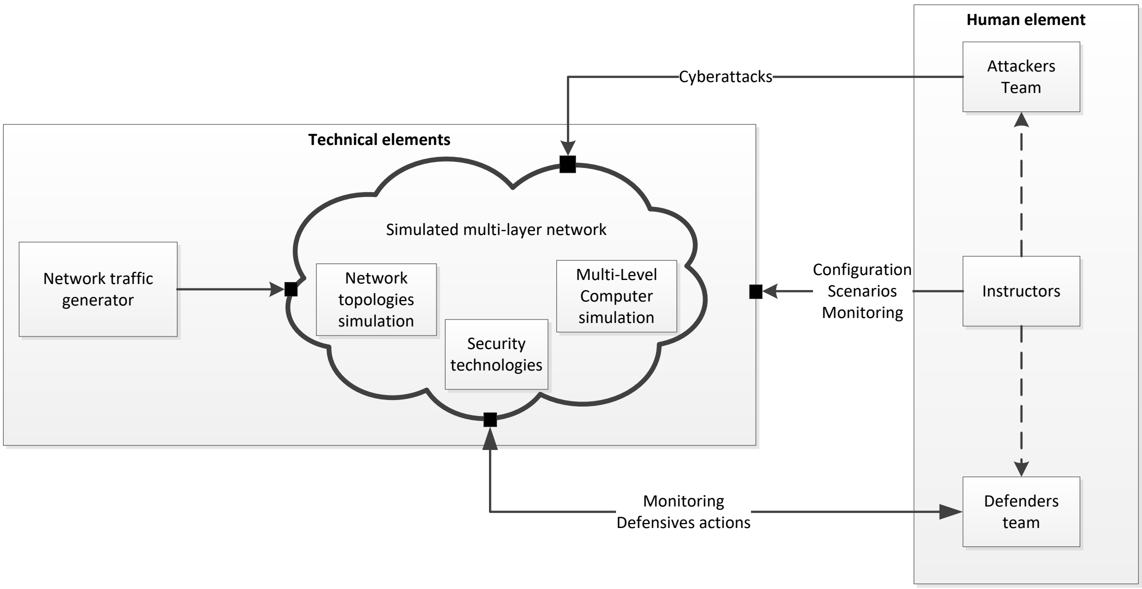
Human element
Attackers Team
Instructors
Defenders team
Cyberattacks
Technical elements
Simulated multi-layer network
Network traffic generator
Network topologies simulation
Multi-Level Computer simulation
Security technologies
Configuration Scenarios Monitoring
Monitoring Defensives actions

Figure 2 CR Eco system

Technically, a CR is characterized by the following elements:

- *A multi-level computer emulation and simulation environment.* Additionally it is called "hybrid" when it allows the connection of physical equipment (router, probe, industrial PLC, etc.) or appliances, see Section 2.1.6.
- *Network topologies.* From the point of view of a CR, it represents the network logical architecture. It defines:
    - the links and their properties such as information from the OSI model level 1 up to 3
        - the network components which they are connected to
        - IP addresses
        - Bandwidth
    - the network components such as switches, routers and their properties:
        - routing process ranging from no routing, direct routing up to dynamic routing with BGP, OSPF, etc.

    - diffusion mode unicast, multicast and even broadcast data flow rate limiting
    - open services like SSH protocol, log management, etc.

- *Security technologies***.** These cover the set of defensive (e.g., firewalls, IPS/IDS, SIEM, etc.) and offensive (NMAP, Kali Linux, etc.) security technologies and tools
- *Network traffic generator.* These generators inject legitimate and illegitimate traffic into the environment to create the "noise" inherent in any network and simulate the realistic operational network traffic.

On a basic human level, CR operations are organized around 3 distinct teams:

- *The "Attackers" often called "Red team(s)",* are composed of professional ethical hackers, generally belonging to the organization of the CR. This team reproduces targeted attacks of scale and increasing complexity, likely to challenge the defence according to its margin of progress throughout the training;
- *The "Defenders" often called "Blue team(s)",* are in charge of the defence of the networks and information systems, and are therefore consisting of the trainees participating in the training/cyber exercise.
- *The "Instructor" sometimes called "White Team",* are both in charge to create the architecture scenario, configure and monitor the work of the other Teams.

The red and blue teams are commonly seen in all CRs based scenarios. More specialized/dedicated teams can include [8]:

- Green team dedicated to the infrastructure;
- Yellow team dedicated to situation awareness;
- White teams dedicated to control and legal support;
- Purple team dedicated to perform communication between multiple exercises;
- Orange team: during exercise, orange team members can assign technical tasks and/or challenges to the blue team members. This gamified approach gives the opportunity to blue team members to earn points after successfully completed the assigned tasks and/or challenges
- Autonomous teams: when automation is used in a scenario for simulating any kind of aforementioned role or teams, we called these teams autonomous teams whatever they are simulating including blue, red or other team

- Grey team dedicated to the maintenance of the normal traffic and service requests.

Moreover, beyond the scenario and exercises, CRs have also to implement content dealing with techniques and procedures. Thus, it could lead the CRs to offer to the trainees the expected knowledge, which is necessary to meet the objectives of the training.

Effective operational training is a key usage and promise of CRs [9]. The overarching aim of operational training aims at cultivating both individual and team skills to the participants of a simulated/emulated attack-defence scenario. Research in this area includes the exploration and systemization of optimal training processes and objectives. A recent study proposed a taxonomy for cyber security training methodologies considering the following two aspects [10]:

(i) the content of the training program

(ii) the associated practical activities

Regarding (i), the study classifies training content in the following, not mutually exclusive classes. Attack-oriented training (including attack techniques like penetration testing, vulnerability exploitation etc.), defence-oriented training (i.e. the design, implementation and usage of defence mechanisms) and analysis/forensics-oriented training which aims at a more systematic understanding of cyber-attacks. The last category involves also the so-called static attacks, which take place before the start of the training. Trainees are then expected to recover and analyze attack traces recorded in the system, in order to find out what kind of attack has been performed. This is in contrast with the dynamic attack scenarios, where attacks take place during training [11].

Regarding (ii) the authors classify training activities as aiming to cultivate individual skills (i.e. packet sniffing, vulnerability scanning etc), team skills and enhanced CSIRT capabilities.

Since CRs are a still evolving domain, both the design of optimal training procedures (including the gamification approach mentioned below) as well as the quantification of their effectiveness remain largely open questions [4], [12], [13].

2.1.5 Simulation

Simulation involves modeling the state of the target. The result of a successful simulation is that the simulation model will emulate the target it is simulating. This technology is mainly used in CR through the use of tools, listed in chapter 0

Cyber range tools, for example: simulate network, SCADA protocol (Traffic generation).

For example: The 3D CAR SIMULATOR or FLY SIMULATOR simulators model as accurately as possible every detail, every behavior of the target to represent what the target does in reality.

2.1.6 Emulation

Emulation is the process of imitating externally observable behavior to match an existing target. The emulation mechanism does not have to reflect accurately the internal state of the target it mimics.

The emulation is mainly used to mimic an electronic materiel. It permits to transform a materiel behavior in software behavior. This technology mainly combined with the virtualization technology.

The emulation technology is used by a lot of tools, listed in section 0

Cyber range tools and it's used in many domains such as Cloud, Critical infrastructure, Hybrid network, IOT, SCADA etc.

2.1.7 Simulation vs Emulation

From research perspective, CRs are expected to provide a reliable testing tool for cyber security products and activities. The reliability of the tests is heavily dependent on how accurately the CR represents the actual network of interest. The two extremes of building such a representation are through simulation or emulation type CRs.

In most cases, CRs simulate/emulate the actual network by utilizing virtual realizations of its components. These realizations may be models (in the case of simulation) and/or components of the physical infrastructure of the cyber range (in the case of emulation), corresponding to actual components of the network under consideration. Emulation type CRs shine in realism of network representation and/or fidelity of the results, are however very expensive. Simulation type CRs excel in scalability and flexibility, may however produce unreliable results.

Depending on the required degree of fidelity of the cyber range compared to the actual network, a mixture of simulating and emulating components can be selected. Current research and development on CR usage includes the case-specific exploration of the most appropriate such mixtures in terms of both fidelity and cost effectiveness [14], [15].

The development of such models, software and/or hardware components able to address the highly complex, multi-parametric and dynamic nature of real network components within a customizable CR interface requires significant effort, and remains an active area of research [3], [4], [16]–[20]. Of particular interest are CRs that regard networks interconnected with Industrial Control and SCADA systems, since they pose a variety of challenges. Such systems are most usually operated and maintained by personnel that is unaware of cyber-attacks; they are extremely expensive to emulate, and the consequences of an attack on such systems may be devastating. Recent attempts addressing this problem include [21], [22] and the SCADA component of the Michigan University cyber range [23].

Theoretically, ad hoc or overlay type CRs offer the best of the two extremes, i.e. emulation/simulation. While taking into account the actual devices present in the network, the overlaid network can be configured at will, in both topology and functionality. However, given the minimal protection provided by the overlay software between the actual and the virtual network, this type of cyber range is not suitable for most activities and therefore it is used more rarely [3].

There are significant advantages and disadvantages to both of these approaches, but in general simulation-based tend to be valued for high scalability on a small number of servers. In comparison, while emulation is more expensive to implement, the simulations are often more realistic. More generic details between simulation and emulation can be found in other research [24]. Some observations on simulation and emulation for cyber security in maritime can be found in [25]. The evolution of the use of simulation end emulation is described in research of J. Davis and S. Magrath, "A Survey of cyber ranges and Testbeds" [7] .

In research paper, "Cyber ranges and security testbeds: Scenarios, functions, tools and Architecture" [2], the simulation and emulation approaches throughout the last fifteen years are presented. Initially, simulation was mostly used in CRs, then the emulation growth in 2005 significantly exceed the simulation by 2010 until today.

Cutting-edge CR technology, based on simulation, has been recently produced by NASA for research related to space stations [26]. The purpose of this CR was to provide cyberwarfare training and technology development. This simulation-based CR provided NASA with an adaptable virtual environment that represented a typical NASA mission system of systems environment. This CR enabled the training of network defenders and the ability to perform simulated red vs blue team training.

Another state-of-the art simulation based solution for studying industrial control systems (ICS) has been presented in [21]. This focused on raising cybersecurity awareness amongst ICS maintenance staff. Similarly, Cyber-MAR aims to raise awareness in the maritime sector. Just as this research aims to address the lack of cost-effective CRs for the industrial domain, so does Cyber-MAR in the maritime sector. Despite the similarities between different domains such as ICS and the space the unique network representations and functionalities require unique CRs configuration and capabilities as well.

With respect to Cyber-Physical systems, research is oriented towards both emulation-based [27] and simulation-based [28] solutions. In the maritime sector [29], cyber-physical systems are becoming more popular and pose a potential risk for cyber safety. Therefore, the security risk assessment of cyber-physical systems is becoming more important. As maritime is nowadays critical to the realization of the world trade, it is paramount that CRs in this niche evolve more quickly to meet cyber needs.

In addition to the categorization of CRs into simulation or emulation based, significant differences in CRs for commercial, government/military, or academic purposes can be identified [8]. Table 6 (See Section 2.3.3) focuses primarily on the commercial CRs, while the following papers focus more on academic and governmental CRs, at least on those known to the public (See Section 2.3.2) [3], [7].

2.1.8 Cyber range tools

CRs functions are implemented in domains such as Cloud, critical infrastructure, hybrid network and Application, IOT, SCADA, autonomous systems. These functions are available by the use of multiple tools listed in [7]and given also below.

- Virtualization/Emulation technology :

Domain	Tools
Cloud	LAAS Cloud infrastructure
	Openstack
Critical infrastructure	EMULAB
	Hyper-V
	NetEM
Hybrid network	Virtualbox
	VMware ESXI
	KVM/QEMU
IOT	Openflow switches
	Vmware Vsphere
	Qemu system
SCADA	Mininet
	Proxmox VE
	Core emulator
Network	Xen-VM
	Open V-Switch
	XORP Router
	Open VZ

Table 1 - Emulation Tools [7]

- Simulation technology :

Domain	Tools
Critical infrastructure	Qualnet
	SCADASim
	Digsilent Power fatory
SCADA	Matlab
	Analog I/O
	Modbus I/O
Network	ModelNet
	NS2, NS3
	Network Simulator
Autonomous system	Qualnet
	Transas

Table 2 - Simulation Tools [7]

- Monitoring Technology:

Domain	Tools
Cloud	Netflow
	IPFIX
Critical infrastructure	Zabbix
	prometheus
	Wireshark
Hybrid network	Nagios
	OSSEC
	Tcpdump
IOT	ADB
	Opendaylight controller
	Wireshark
SCADA	SNORT
	BRO IDS
	Can analyzer
Network	Testbed@twisc Monotor
	Traceroute
	Suricata

Table 3 - Monitoring Tools [2]

- Traffic generation:

Domain	Tools
Cloud	Low Orbit Ion
Critical infrastructure	Modbus
	DITG
	Open flow
Hybrid network	ISEAGE
	Traffic Collector replayer
IOT	Printer
	Microworks
	SNMP
SCADA	Traffic fuzzer
	MODBUS
	DNP3
Network	Hydra
	Emulab
	tfn2k

Table 4 - Traffic generator Tools [7]

2.2 Cyber-range technologies

As discussed in previous sections, a CR is providing a simulation of ICT and/or OT environments to be used for a wide range of purposes and it is both hardware and software. The following sections present the main technologies integrated in CR.

2.2.1 Architecture

The software architecture of a CR is based on the use of a hypervisor solution such as the KVM hypervisor[1] with regards to the virtualization of systems. A host virtual machine such as Qemu[2] is responsible for running the emulation layer if necessary, this happens when an ARM purposed virtual machine on servers of in x86 architecture.

The CR can also use a containerization technology based on Linux containers such as LXC[3]

The orchestration of all these technologies is provided by a tool such as libvirt[4] . Libvirt is collection of software that provides a convenient way to manage virtual machines. A network topology is made up of connections between the virtual machines defined in the CR. These connections are links at level 2 of the network stack. The switches can be implemented in two different ways. These are either simple TAP linux or if more configuration setups are required it can be an open-vswitch[5] switch. This allows to define vlan on switches.

The hybrid capacities of the platform are provided by the physical Ethernet plugs present on the servers. The only limitation that exists on such a platform is related to the number of virtual machines that can be defined on a server. It is therefore possible to add as many servers as necessary. The platform is made up of a master responsible for orchestrating a set of nodes.

[1] https://www.linux-kvm.org/page/Main_Page
[2] https://www.qemu.org/
[3] https://linuxcontainers.org/ .
[4] https://libvirt.org/
[5] http://www.openvswitch.org/

2.2.2 The tools used within a CR

From a technological perspective, a CR is agnostic i.e. anything that can be virtualized can be used in this virtual version. What is not feasible to be virtualized can be connected in real to the CR. It is therefore possible to use in any network topology the security solutions present on the market.

For licensing reasons, the open-source solutions of a product are preferred. The most common solutions that are used are the following:

- Firewall: solutions such as pfsense[6]
- IDS: solutions such as SURICATA[7]
- IPS/IDS: frameworks such as SELKS.

2.2.3 Traffic generator.

Traffic generation is an essential building block of a CR because it realizes all the events that should be simulated to a defined topology. As part of an exercise its use makes it possible to hide malicious network frames among a legitimate frame stream. This results in more realistic exercises and training sessions.

There are several technologies to provide such type of functionality:

- TRex[8] is the traffic generator developed by CISCO under an Apache open-source license. It consists of a software product which can be installed in a virtual machine within the CR
- Cyber Test System[9] offers a hardware traffic generation solution.
- BreakingPoint produced by IXIA[10] is a solution that can be both hardware and software. products/network-security-testing-breakingpoint

2.2.4 SIEM

Security Information and Event Management systems (SIEMs) are tools designed to collect events coming from multiple sources within a monitored infrastructure. They generate correlated alarms that indicate an anomaly in the system and help security administrators in identifying possible threats and attacks against the protected infrastructure [30].

Generally, a simple SIEM is composed of separate blocks (e.g., source device, log collection, parsing normalization, rule engine, log storage, event monitoring) that can work independently from each other, but without them all working together, the SIEM

[6] https://www.pfsense.org/
[7] https://suricata-ids.org/
[8] https://trex-tgn.cisco.com/
[9] https://cybertestsystems.com/
[10] https://www.ixiacom.com/

does not function properly [30]. Figure 3 depicts the basic components of a regular SIEM solution.

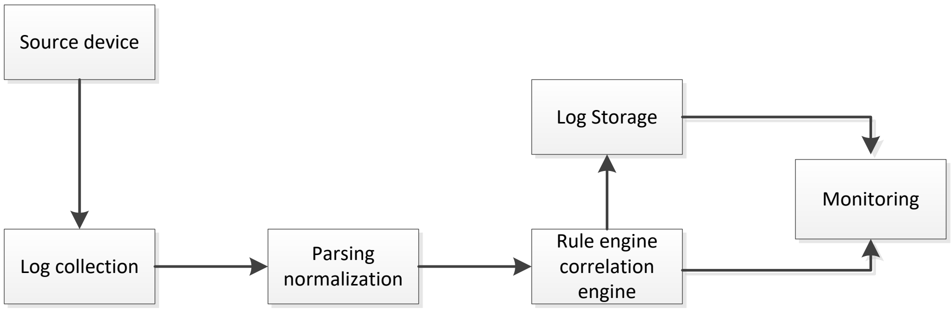

Figure 3 - SIEM basic components

Besides the aforementioned capabilities of SIEMs, there are many differences between the existing systems that normally reflect the different positions of SIEMs in the market. While some of them are more focused on detection and alert correlation, some others are providing new capabilities for user behaviour, visualization, storage and reaction.

2.2.4.1 SIEM Classification

Analysis and evaluation of security systems have been widely proposed in the literature. While some research focuses on the commercial aspects, others concentrate on the technical features that could be improved in current SIEM solutions. Well known institutions like Gartner[11], for instance, propose a commercial analysis of SIEM systems based on the market and major vendors, for which, a report is released on an annual basis to position SIEM vendors as market leaders, challengers, niche players or visionaries.

Other security institutions (e.g., Techtarget [31], Info-Tech Research Group [32]), have widely reported on the capabilities of SIEM solutions and on the way SIEM vendors can be compared and assessed. Techtarget, on the one hand, releases periodic electronic guides about securing SIEM systems and how to define SIEM strategy, management and success in the enterprise [33]. Info-Tech, on the other hand, provides technical reports on the SIEM vendor landscape [34] focusing on the benefits and drawbacks of major commercial SIEMs. Both organizations take the Gartner Magic Quadrant[12] as the baseline for their analysis.

[11] https://www.gartner.com/en
[12] https://www.gartner.com/en/research/methodologies/magic-quadrants-research

During the last decade, Gartner has classified SIEM solutions as (i) Leaders: organizations that execute well against their current vision and are well positioned for the near future; (ii) Visionaries: organizations that understand where the market is going or have a vision for changing market rules, but do not yet execute well; (iii) Niche Players: organizations that focus successfully on a small segment or are unfocused and do not out-innovate or outperform others; and (iv) Challengers: organizations that execute well today or may dominate a large segment, but do not demonstrate an understanding of market direction.

Table 5 shows the current Magic Quadrant for available SIEM solutions.

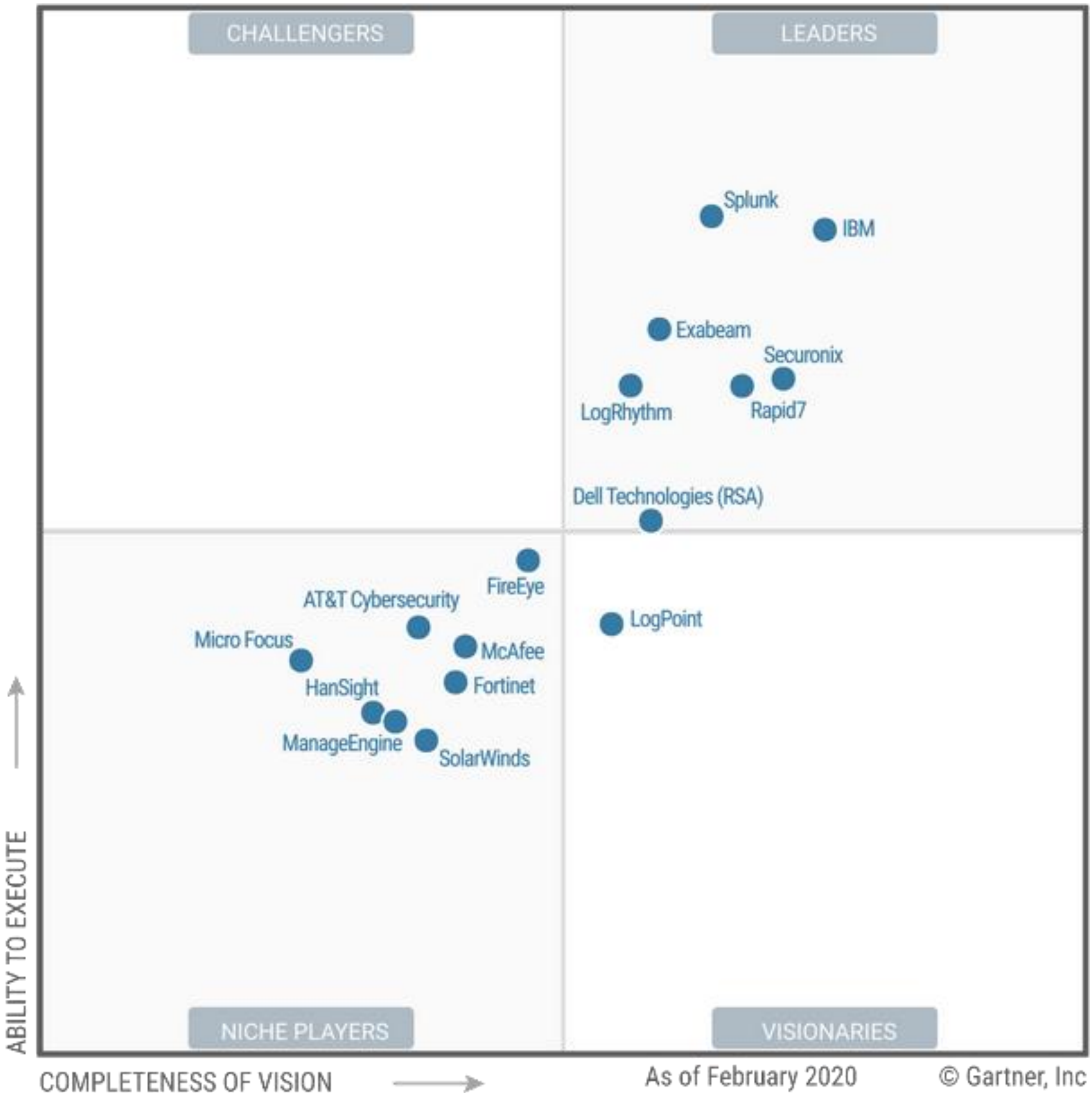

Table 5 - SIEM Vendors Gartner Classification Source: Gartner (February 2020)

An important aspect to note is that some SIEM vendors have been in the top Gartner classification list since they first appeared in the market (e.g., Splunk[13], AlientVault[14], SolarWinds[15], EventTracker[16], Fortinet[17], BlackStraus[18], Micro Focus[19]). Some others have joined the list in the past couple of years with User and Entity Behavior Analytics (UEBA) features (i.e., Manage Engine[20], Venustech[21], Rapid7[22], Exabeam[23], Secureonix[24], and LogPoint[25]). A recent study [35] considers 22 players in the 2020 SIEM vendor map based on three main capabilities: (i) threat intelligence detection, (ii) compliance, and (iii) log management. Figure 4 depicts this information.

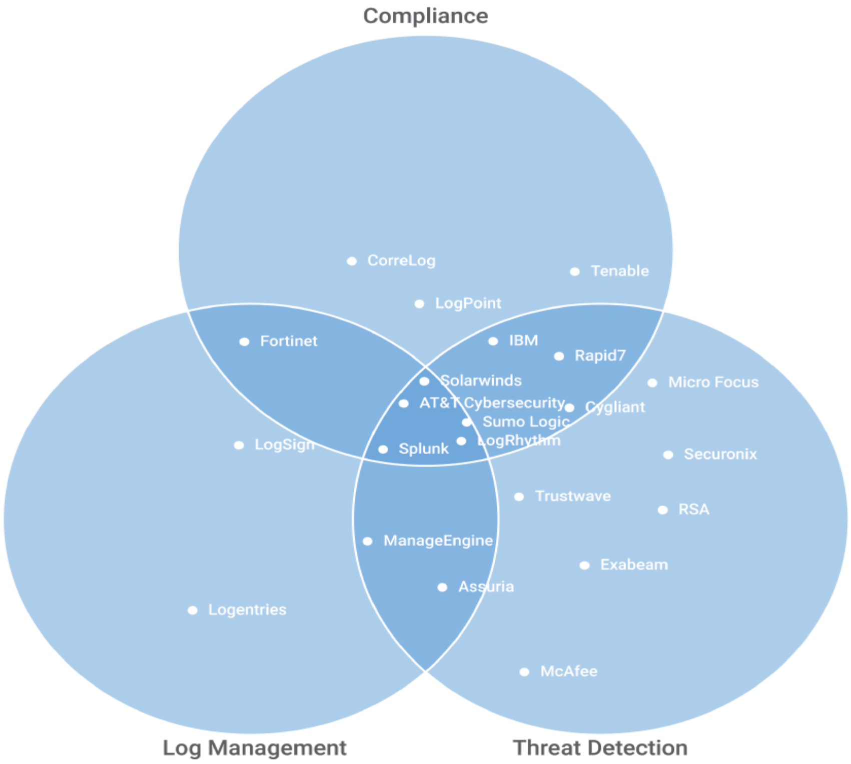

Figure 4 - 2020 SIEM Vendor Map Source: Solutions Review – 2019 SIEM Vendor Map

[13] https://www.splunk.com/en_us/siem-security-information-and-event-management.html
[14] https://cybersecurity.att.com/products/usm-appliance
[15] https://www.solarwinds.com/security-event-manager
[16] https://www.eventtracker.com/
[17] https://www.fortinet.com/products/siem/fortisiem.html
[18] https://www.blackstratus.com/siem-security-solutions/
[19] https://www.microfocus.com/en-us/products/arcsight-express-siem-appliance/overview
[20] https://www.manageengine.com/products/eventlog/?pos=MEtab&cat=ITS&loc=tab&prev=AB2
[21] http://venusense.com/product/view/11165.html
[22] https://www.rapid7.com/products/insightidr/
[23] https://www.exabeam.com/product/
[24] https://www.securonix.com/products/securonix-next-generation-siem/
[25] https://www.logpoint.com/en/

Besides threat intelligence, compliance and log management, SIEM developers are considering User and Entity Behavior Analytics (UEBA) capabilities and smart dashboards as innovations to be added to their solutions. As a result, new SIEM systems will help security administrators with pre-built dashboards, reports, incident response workflows, advanced analytics, correlation searches and security indicators [36]. In addition, an in-depth analysis of SIEMs extensibility [37] revealed that current SIEM solutions need to improve features such as behavioral analysis, risk analysis and deployment, visualization, data storage and reaction capabilities, in order to keep up with the market.

2.2.4.2 SIEM Tools

Considering the previous information about SIEMs, Table 6 summarizes some of the most promising SIEM tools up to date.

SIEM	Advantage	Limitation
Splunk[26]	- Market-leading platform in Operational Intelligence. - Offers data collection, indexing, and visualization capabilities for security events monitoring - Uses advanced security analytics, which include both unsupervised machine learning and user behavior capabilities.	- Uses basic predefined correlation rules for monitoring and reporting requirements. - Reaction capabilities are limited to email notifications. - Requires integration with third-party applications for task and workflow automation.
LogRhythm[27]	- Provides end-point monitoring, network forensics, user and entity behavior analytics, and response capabilities. - Can be deployed in an appliance, software or virtual instance supporting scalable decentralized architectures	- Unsuitable for organizations with critical infrastructures although extensions can be deployed to enhance the SIEM capabilities. - Requires high degree automation and out-of-the-box content
Dell technologies (RSA)[28]	- Analyzes data and behavior of people and processes within a network across a company's logs, packets and end-points. - Focuses on advanced threat detection. - Provides strong OT monitoring capabilities	- Although the number of technical components and the licensing models provide extensive flexibility in designing the deployment architecture, it requires understanding of the breadth of the options and the implications for cost, functionality and scalability.
Exabeam[29]	- Allows collecting unlimited log data, use behavioral analytics to detect attacks, and automate incident response.	- Lack of cloud support for its analytics solution as a SaaS model, limiting applicability for some organizations.

[26] https://www.splunk.com/en_us/siem-security-information-and-event-management.html

[27] https://logrhythm.com/solutions/security/siem/

[28] https://www.rsa.com/en-us/products/threat-detection-response/siem-security-information-event-management

[29] https://www.exabeam.com/product/

SIEM	Advantage	Limitation
	- Provides granular role-based data access and workflow to support privacy concerns. - Provides mature user behavior analytics (UBA) capabilities.	
IBM Qradar[30]	- Can be deployed as a hardware, software or virtual appliance, as well as a Software as a Service (SaaS) on the IBM cloud. - Provides a user interface for real-time event and view, reports, offenses, asset information, and product management. - Offers support for threat intelligence feeds.	- Provides basic reaction capabilities that include reporting and alerting functions. - The endpoint monitoring for threat detection and response, or basic file integrity requires the use of third-party technologies.
AT& T Cybersecurity[31]	- Offers both: commercial solutions (i.e., Alienvault Unified Security Management - USM[32]) and open source SIEM solutions. (i.e., OSSIM[33]). - Includes a web-based graphical interface for administration, reporting and security event management.	- Limited user or entity behavior analytics as well as machine learning capabilities. - Basic reaction capabilities (e.g., send email, execute script, open ticket) and limited to the pre-defined set of conditions associated to a security policy.
Micro Focus[34]	- Offers two SIEM solutions: Micro Focus ArcSight (after HPE[35] joined Micro Focus) and Micro Focus Sentinel (after NetIQ joined Micro Focus). - Provides a graphical interface for the Security Operations Center (SOC) team and a set of applications or external commands that help the correlation and/or investigation processes.	- Limited visualization options and intricate correlation rules [38]. - The information associated with events is immutable, with evident deficits when it comes to adapting the product to company processes and needs.

[30] https://www.ibm.com/security/security-intelligence/qradar
[31] https://cybersecurity.att.com/
[32] https://cybersecurity.att.com/products
[33] https://cybersecurity.att.com/products/ossim
[34] https://www.microfocus.com/en-us/home
[35] https://www.hpe.com/emea_europe/en/home.html

SIEM	Advantage	Limitation
Fortinet[36]	- Can be deployed as a single appliance or as individual, stand-alone components for scalability. - Provides complementary SIEM features that include a built-in configuration management database (CMDB), application and system performance monitoring. - Comprises visibility, cross-correlation, automated response and remediation in a single, scalable solution.	- Analytics are a work in progress. - Lag behind many competitors in the use of advanced analytics, such as using Machine Learning.
Solarwinds [37]	- Provides centralized log collection and normalization, automated threat detection and response, intuitive visualization and user interface, as well as real time correlation and log searching to support investigation.	- Lacks support for monitoring public cloud services' IaaS or SaaS - Does not support custom report writing and customization of out-of-the-box compliance report templates.

Table 6 - SIEM Tools

[36] https://www.fortinet.com/products/siem/fortisiem.html

[37] https://www.solarwinds.com/security-event-manager

2.3 Panorama of cyber range

2.3.1 Federated cyber ranges

According to [3], both the accuracy of network incident representation plus capability to replicate a cyber security exercise at desired scales are crucial for cyber range technology. However, there seems to be a trade-off between the accuracy of representation and the scalability of a CR. Virtualization does not solve the problem, since multiple virtual machines on a single physical one impairs the fidelity of the network representation, due to contention for resources. Furthermore, due to the wide variety of different kinds of contemporary networks plus the fact that many of them operate on a large scale, any attempt to satisfy both these demands can very quickly become cost-inefficient and complex from a technological point of view.

A current research trend aiming to address this issue is the interconnection of different CRs, in order to create federated CRs with shared infrastructure. However, integration of and interconnection of different CRs appears to be a non-trivial task, requiring a carefully developed test plan to ensure the proper connectivity of each device [4]. Such attempts include the aforementioned NCR, CRATE and NATO CRs plus work in [39], [40]. Shared infrastructure between individual CRs with different specialization (e.g. ICS, SCADA, computer networks) can provide shared capabilities and an increased cyber attack surface, thus replicating actual cyber incidents with greater consistency.

An indicative example of federated CRs is the European Defence Agency's (EDA) CRs Federation project with 11 Member States of the EU participating in it [41]. The aim is to connect existing national CRs for training purposes and improving cyber defence skills.

2.3.2 Panorama of academic and research cyber-range and State of the art cyber range facilities

There are several state of the art CRs in the academic sector. The Michigan CR is one of the most advanced [42]. The Michigan CR offers a platform of cyber security exercises and simulation scenarios that have been used for the education of students and a wide variety of professionals. The Regent cyber range was established in 2017 [43]. It is fully customizable and provides a variety of virtualization capabilities required in training scenarios. It also provides several state of the art capabilities, including a threat identification module, monitoring and event management systems plus risk assessment and forensics tools. Other CRs in the academic sector include the Arkansas, Wayne State, Florida and Virginia CRs [44]–[47].

In the defence/military sector, the NATO and the National CR (NCR developed by DARPA) CRs are the most notable CRs [48], [49]. One of the largest annual defence exercises, namely 'Cyber Coalition' is conducted in the NATO cyber range facilities. The NATO cyber range offers a variety of capabilities including simulated electronic warfare and rehearsal scenarios. The NCR cyber range is maintained by the Defence Advanced Research Projects Agency in order to provide a national level virtual platform for cyber security exercises. It is designed to provide a high fidelity-high flexibility platform that supports fast configuration and reliable evaluation of cyber security products and activities [4]. The capabilities of the NCR cyber range include network traffic generators and trackers, plus a variety of tools for modeling real world applications and network attacks. The CR and Training Environment (CRATE) is developed and maintained by the Swedish Defence Research Agency [50]. Its physical infrastructure consists of about 800 servers, which can be configured as needed, and supports a large number and variety of deployable operating systems and applications. CRATE also provides tools for simulation, intrusion detection and facilitates vulnerability detection. The Department of Defence (DoD) also provides a rich set of capabilities, including a modeling and simulation environment, and tools for penetration testing, requires however a quite tedious manual event configuration and is not very scalable [51].

The following Table as demonstrated in a recent research work [8] summarizes and extents had has been discussed above:

Cyber range	Federate	Public	Private
NCR	Y	N	N
Michigan	Y	Y	Y
Virginia	N	Y	Y
IBM	N	N	Y
CRATE	Y	N	N
Cisco	N	Y	Y
UD	N	N	Y
NATO	Y	N	N
CourrierDOD	Y	N	N
Raytheon	Y	N	N
Baltimore	N	Y	Y
Florida	Y	Y	Y

Table 7 - Academic and research cyber-ranges [8]

Several reviews and surveys of CRs and industrial control-system (ICS) security testbeds have been performed in the past, for example:

- Davis and Magrath [3] present one of the first extensive reviews of existing military, academic, and commercial CRs. However, since the review is based solely on publicly available information, they remark that their review may not be comprehensive. They found that main roles for the CRs are testing, training, research and development, while training being the most popular role. They categorize CRs into three categories by their implementation approaches: simulation, emulation and overlayed CRs on top of live production systems. The reviewed CRs mainly use the simulation or the emulation approach. Simulation is cost-effective and scalable but suffers from lower fidelity due to simulation models often being very high-level abstractions of their real-life counterparts. Emulation, on the other hand, is able to provide high fidelity and repeatability as the result of using real software and hardware instead of models. Yet, it is more expensive and does not scale as well as simulation. However, emulation cost can be reduced by using virtualization and resource sharing. Authors further note that hybrid approaches combining emulation and simulation to combine best aspects of the both approaches are gaining popularity.

- Holm et al. [52] survey Industrial Control-System testbeds used for scientific research. Their work identifies 30 different testbeds, most of which are designed for vulnerability analysis, education, or testing. They study how different areas of ICS systems, i.e., control-center, communication network, field devices, and physical processes, are implemented in the testbeds and how virtualization could be utilized in their implementation. They argue that field devices are the hardest area to virtualize due to lack of support from virtualization platforms.

- In their work, Vykopal et al. [53], present a systematic literature review of advances in CRs and testbeds between years 2013 and 2017 to close the gap after Davis's and Magrath's work. They identify around 30 CRs, most of which focus on cyber security training and education. The review indicates a rapid rise of cloud-based CRs and use of virtualization and containers to provide an isolated environment. They further discuss high-level requirements and architecture for their cloud-based KYPO CR. Among the requirements they include flexibility of supported network topologies and software systems, scalability of the cyber range, balance between isolation and interoperability (extensibility) with external systems, cost-efficiency, built-in monitoring, as well as ease of access.

- Kavallieratos et al. [28] presents a survey of 32 cyber-physical systems testbeds in five different application domains, including ICS/SCADA testbeds. All the discussed security testbeds also aim to contribute towards security training. They discuss limitations and challenges of the existing testbeds. For example, software-based solutions offer cost-effective and flexible implementations, but they cannot be used to implement many physical attacks. Based on their survey they note that implementations consisting of a mix of virtual, simulated, and real components appear to be the best option for cyber-physical systems. They further define high-level requirements for a cyber-physical range, i.e. a cyber range for cyber physical systems, based on Vykopal et al.'s [53] work. Main additions are adaptability of the cyber range configuration to different cyber-physical systems with reasonable effort and shareability of individual components. In addition, Kavallieratos et al. present reference architecture for a cyber-physical range and provide an example instantiation of the architecture in a form of a Cyber-enabled ship testbed for validating attack scenarios in ship infrastructure.

- Ani et al. [54] present a systematic review of 41 ICS security testbed articles with the goal of identifying design factors that contribute to testbed's credibility, i.e., confidence, trustworthiness, and acceptability of the testbed as a correct representation of a real system and suitability to its use. They find five contributing factors. First, clearly defined security-related design objectives and security scenarios guide architectural design, attributes, and decisions and help to maintain focus. Second, clarification of the implementation approach (e.g. simulation, emulation) and the used degree of abstraction helps in understanding and validation of testbeds capabilities. Third, demonstrating testbed's core characteristic (i.e., high-level requirements by Vykopal [53] and Kavallieratos [28])helps to establish credibility, though, the right balance between the different characteristics depends on the testbed's core objectives. Fourth, the scope of the architectural components covered by the testbed architecture contributes toward credibility of fidelity and quality claims. Finally, addressing testbed evaluation process can increase testbed's credibility in the eyes of others. Based on their findings Ani et al. develop an ICS testbed credibility-building process that can be used to apply identified factors into a testbed implementation.

- Yamin et al. [7] provide systematic literature review of 100 cyber range and security testbed related publications and develop a taxonomy to classify generic capabilities and functionality of CRs.

- A recent master's thesis by Chaskos's [55] reviews 16 CRs and their capabilities. Based on these, the thesis aims to describe a, federated, state-of-the-art cyber range for cyber security training.

Open-source tools to support the basic CR operations have emerged also. For example, the open-source Cyber rangeproject[38], in which the CR is fully deployed in the AWS cloud platform. The goal of the project is to provide an AWS-based environment for offensive/defensive training quickly for different educational purposes. While it is providing an easy-to-setup environment, it does not fit directly for a user that wants to run a local setup of their environment in the cyber range.

2.3.3 Panorama of the market

This Section shows a panorama subset of the main actors of the market. It is important to distinguish between the technology suppliers and the providers of training and

[38] https://github.com/secdevops-cuse/CyberRange

training within an internal framework (e.g., a Ministry of Defence or a university) or for the benefit of external clients.

Technology Providers, different equipment manufacturer's offer CRs or simulation environments dedicated to cybersecurity (see Table 8 - Technology providers below).

Enterprise	Country	Sector	Service
Cyberbit (ELBIT Systems)	Israel	-Public sector -Service Providers -Academic World -Organizations	-Training for business leaders -Use of SCADA hardware + ICS / SCADA protocol -Scenarios tailored to customer needs
Cyber Test Systems	France	-Network Equipment Manufacturers -High Service Providers Speed and mobile -System Integrators -Companies -Defence Contractors -Governments	-Technology: generator trafficking case legitimate and malicious (Cyber-Test Systems -Network Traffic Generator - CTS-NTG), associated a software solution in charge of control of the housing -Scenarios including attacks ICS / SCADA DDoS attacks, DoS, botnet command-and-control (C & C) communications, etc.
Ixia	United States	-Cyber-Warriors -Public Organizations -Companies wishing to defend their critical infrastructure, their society and their network	-Platform all-in-one test security and performance -Education and training of staff to practical exercises within levels increasing difficulty
Oracle (Ravello Systems)	United States	-Enterprises	-On-demand CR -Technology: Virtual Clone Network (VCN) totally isolated and independent Internet -Solution: clone the corporate network in the Cloud rather than using the current network
Sypris	United States	-Private sector -Owners and operators information infrastructure critics	-Modeling and simulation to configure customizable virtual environments, from a single server to an extranet/Web interface -API that allows the extension of the functionalities by a third party -Virtual Training Platform (VTP)
Diateam	France	-Initially on behalf of the DGA -Now open to players public and private	-HNS Platform (Hybrid Network Simulation) suitable for forming and driving the cyber, the management of cyber-attacks, the ICS / SCADA extensions
Airbus	France	Aerospace, Aeronautic	- Realistic Simulation: Immersion in complete IT/OT systems and animation

Enterprise	Country	Sector	Service
			with a complex scenario framework
Boeing	United States	-Governments -Industry customers	-CR-in-a-Box (CRIAB) -CRIAB allows modeling and simulation of complex missions and advanced threats.
JYVSECTEC	Finland	-Several	JYVSECTEC is an independent cyber security research, development, and training center. [39] -Realistic Global Cyber Environment (RGCE) offers live cyber range -RGCE combines virtualization techniques, physical devices, and business specific systems
CybExer Technologies	Estonia	-Various organizations	- CybExer Range Platform that supports on-premise or CybExer range exercises. [40] - Pay-as-you-go service - Exercise environment creation and automated deployment, customized scenario and game net creation for exercises. - Integrated Scoring and Awareness tool (ISA).
Accenture	Ireland	-Industrial companies	Three CRs[41] in different locations focusing on: -the oil and gas industry, -utilities industry from electric transmission to distribution, -utilities and chemicals industries focused on electric distribution networks and chemical plants.

Table 8 - Technology providers

[39] https://jyvsectec.fi/services/exercises/overview/
[40] https://cybexer.com/#range
[41] https://newsroom.accenture.com/news/accenture-expands-cybersecurity-capabilities-with-network-of-CRs-to-help-industrial-companies-simulate-and-respond-to-cyberattacks.htm

3. Beyond SotA

Additional CR-related research trends concern the introduction and implementation of various additional functionality enhancing features to the cyber range technology, which are detailed below.

Analyzing cyber-threats can unravel several aspects of pertinent incidents [10], [56]. Contemporary cyber threats can potentially utilize a variety of means for infiltration and propagation in a vulnerable network, and do so in multiple stages [57]. An intelligence module able to collect and process pertinent data would be a reasonable addition to expect in cyber range technologies, and there are several commercial examples up to now including the IBM X-Force Incident Response and Intelligence Services (IRIS) and GECI Cyber Solutions [58], [59].

At all levels, cyber security practice involves the compilation and preservation of attack-related evidence, in order to investigate the current state of a system and potentially reconstruct a sequence of suspicious events [60]. Therefore, many state-of-the-art CRs include a forensic evidence module [61]–[63].

Situational awareness is also a highly appreciated feature in cyber range technologies [64]. Combined with a visual analytics module it provides the actors with the ability to make real-time informed decisions [13]. The output of a situational awareness module could be also fed to a threat forecasting feature, for detecting anomalies in the network traffic and facilitating remediation [65].

According to the Institute of Standards and Technology (NIST), real time decision making, defence planning and prioritization of defensive actions requires risk analysis. Therefore, efforts are being made to include risk analysis and assessment tools within cyber range technologies [43], [66].

The modern cyber security landscape is continuously evolving and threats can take various and ever changing forms. Therefore, to enhance the awareness, adaptability and creative thinking of cyber security professionals it is important to adopt a dynamic training process, which focuses on cultivating the aforementioned skills to meet challenges in a rapidly changing environment. This is where the concept of gamified training or simply gamification comes at play. The concept of gamification has been described as "the use of game design elements in non-game contexts" [67]. Gamification is an emerging research and experimentation field in cyber security concepts [68], [69]. Pertinent training methodologies include a wide range of training scenarios, from simple, non-expert games, 'Capture the Flag' competitions to complete training ecosystems for cyber-security professionals, aiming to cultivate alertness and creative reactions to the trainees, rather than static knowledge based on previous experience. However, since CRs are virtual representations of real critical infrastructures and they are still isolated from the real network, the challenge remains to design and implement cyber security scenarios that match the corresponding actual real-life situations [1].

Evaluation of CR’s credibility compared to its real-life equivalent is an interesting future research topic. For example, Ani et al. [54] present a systematic literature review of 41 articles that aims to identify which factors contribute to credibility of industrial control systems security testbeds. Their study shows that testbed creators most commonly focus on fidelity, i.e., correlation between testbed simulation and real world observations, but that more than half of the reviewed publications lack any form of evaluation (verification, validation or accreditation) of their testbeds' credibility. In their earlier survey Holm et al. [52] also recognize the need for this kind of evaluation.

Cost-efficient deployment of at-scale security testbed has been a recurring topic in related research and is expected to stay so in the future. For example, one of the main goals of early work by Davis and Magrath [3] was to identify cost-effective ways to obtain at-scale CRs. They viewed emulation as the most promising cyber range implementation method, as it enables high fidelity, but also noted the disadvantage of potentially higher cost compared to simulation. However, they argued that one way to reduce the higher cost is by using virtualization and resource sharing. The authors also noted that federation as a means for cost sharing has been a trend in building network testbeds and assumed that CRs will assume the same approach in the future. A more recent work of Yamin et al. [7] supports this view.

4. Conclusions

This deliverable describes the State of the art Cyber-range technologies analysis, which will serve as an input for the next deliverables "2.2 User requirements related to efficiency, performance, trust, privacy and security ", "2.3 Cyber-MAR System Requirements and Functional specifications" and "2.4 Cyber-MAR System Design and Integration Plan".

It presents the characteristics of the state of the art cyber-rangers, by listing the different classifications and tools, and present key concepts like simulation versus emulation.

It appears that Cyber-MAR would have at least these modules: Intelligent module to collect process and pertinent data, Forensic module, Situational awareness module, Risk analysis and assessment tools, Implementation scenarios real life.

A reflection about Operational technologies hybrid (real/virtual) coupling is also required in order to expand cyber-ranges capabilities for being closer to the realistic industrial maritime environment. It will be described in the deliverable "3.1 OT real/virtual coupling". This document focuses also on the importance of the evaluation of such system and platform cyber-range, which should be taken into account from the design of Cyber-MAR in order to facilitate the global testing strategy.

5. References

[1] W. Newhouse, S. Keith, B. Scribner, and G. Witte, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-181, Aug. 2017. doi: 10.6028/NIST.SP.800-181.

[2] E. W. Ecso, “Understanding Cyber Ranges: From Hype to Reality,” p. 31.

[3] J. Davis and S. Magrath, “A Survey of Cyber Ranges and Testbeds,” p. 38.

[4] V. E. Urias, W. M. S. Stout, B. Van Leeuwen, and H. Lin, “Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper,” in *2018 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2018, pp. 1–5, doi: 10.1109/CCST.2018.8585460.

[5] L. Pridmore, P. Lardieri, and R. Hollister, “National Cyber Range (NCR) automated test tools: Implications and application to network-centric support tools,” in *2010 IEEE AUTOTESTCON*, Sep. 2010, pp. 1–4, doi: 10.1109/AUTEST.2010.5613581.

[6] S. W. Neville and K. F. Li, “The Rational for Developing Larger-scale 1000+ Machine Emulation-Based Research Test Beds,” in *2009 International Conference on Advanced Information Networking and Applications Workshops*, May 2009, pp. 1092–1099, doi: 10.1109/WAINA.2009.183.

[7] M. M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” *Computers & Security*, vol. 88, p. 101636, Jan. 2020, doi: 10.1016/j.cose.2019.101636.

[8] I. Priyadarshini, “Features and architecture of the modern cyber range: a qualitative analysis and survey,” Thesis, University of Delaware, 2018.

[9] “3 Lessons That Are Informing the Next Generation of the Cyber Range,” *Security Intelligence*, Oct. 15, 2018. https://securityintelligence.com/3-lessons-that-are-informing-the-next-generation-of-the-cyber-range/

[10] R. Beuran, K. Chinen, Y. Tan, and Y. Shinoda, “Title Towards Effective Cybersecurity Education and Training,” 2018.

[11] C. H. Pham, D. Tang, K. Chinen, and R. Beuran, “CyRIS: a cyber range instantiation system for facilitating security training,” in *SoICT ’16*, 2016, doi: 10.1145/3011077.3011087.

[12] J. Vykopal, M. Vizvary, R. Oslejsek, P. Celeda, and D. Tovarnak, “Lessons learned from complex hands-on defence exercises in a cyber range,” in *2017 IEEE Frontiers in Education Conference (FIE)*, Oct. 2017, pp. 1–8, doi: 10.1109/FIE.2017.8190713.

[13] R. Ošlejšek, J. Vykopal, K. Burská, and V. Rusňák, “Evaluation of Cyber Defense Exercises Using Visual Analytics Process,” in *2018 IEEE Frontiers in Education Conference (FIE)*, Oct. 2018, pp. 1–9, doi: 10.1109/FIE.2018.8659299.

[14] R. Chertov, S. Fahmy, and N. B. Shroff, “Emulation versus simulation: a case study of TCP-targeted denial of service attacks,” in *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.*, Mar. 2006, pp. 10 pp. – 325, doi: 10.1109/TRIDNT.2006.1649164.

[15] J. Mirkovic, S. Fahmy, P. Reiher, and R. K. Thomas, “How to Test DoS Defenses,” in *2009 Cybersecurity Applications Technology Conference for Homeland Security*, Mar. 2009, pp. 103–117, doi: 10.1109/CATCH.2009.23.

[16] S. von Solms and S. W. Peach, “The design and implementation of a network simulation platform,” in *2013 International Conference on Adaptive Science and Technology*, Nov. 2013, pp. 1–8, doi: 10.1109/ICASTech.2013.6707514.

[17] S. Chapman, R. Smith, L. Maglaras, and H. Janicke, “Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?,” *Journal of Sensor and Actuator Networks*, vol. 6, no. 3, p. 16, Sep. 2017, doi: 10.3390/jsan6030016.

[18] S. K. Damodaran and J. M. Couretas, “Cyber modeling & simulation for cyber-range events,” in *Proceedings of the Conference on Summer Computer Simulation*, Chicago, Illinois, Jul. 2015, pp. 1–8 [Online].

[19] M. Ficco and F. Palmieri, “Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios,” *Journal of Systems Architecture*, vol. 97, pp. 107–129, Aug. 2019, doi: 10.1016/j.sysarc.2019.04.004.

[20] D. L. Bergin, “Cyber-attack and defense simulation framework,” *Journal of Defense Modeling & Simulation*, vol. 12, no. 4, pp. 383–392, Oct. 2015, doi: 10.1177/1548512915593528.

[21] V. Giuliano and V. Formicola, “ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems,” *arXiv:1909.01910 [cs, eess]*, Sep. 2019 [Online]. Available: http://arxiv.org/abs/1909.01910.

[22] B. Hallaq, A. J. P. Nicholson, R. R. Smith, L. A. Maglaras, H. Janicke, and K. Jones, “CYRAN: A Hybrid Cyber Range for Testing Security on ICS/SCADA Systems,” 2017, doi: 10.4018/978-1-5225-1829-7.ch012.

[23] meritmain, “Michigan Cyber Range to Debut SCADA Security Training Component – Merit.” https://www.merit.edu/michigan-cyber-range-to-debut-scada-security-training-component/

[24] T.-S. Chou, S. Baker, and M. Vega-Herrera, “A Comparison of Network Simulation and Emulation Virtualization Tools,” 2016, doi: 10.18260/p.26285.

[25] K. Tam, K. Forshaw, and K. D. Jones, “Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities,” 2019, doi: 10.24868/icmet.oman.2019.005.

[26] B. Bailey, “NASA IV&V’s Cyber Range for Space Systems,” Feb. 25, 2019, [Online]. Available: https://ntrs.nasa.gov/search.jsp?R=20190001085.

[27] A. F. Browne, S. Watson, and W. B. Williams, “Development of an Architecture for a Cyber-Physical Emulation Test Range for Network Security Testing,” *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2882410.

[28] G. Kavallieratos, S. K. Katsikas, and V. Gkioulos, “Towards a Cyber-Physical Range,” in *Proceedings of the 5th on Cyber-Physical System Security Workshop*, Auckland, New Zealand, Jul. 2019, pp. 25–34, doi: 10.1145/3327961.3329532.

[29] K. Tam and K. Jones, “Factors Affecting Cyber Risk in Maritime,” in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Jun. 2019, pp. 1–8, doi: 10.1109/CyberSA.2019.8899382.

[30] D. R. Miller, S. Harris, A. Harper, S. VanDyke, and C. Blask, *Security Information and Event Management (SIEM) Implementation*. McGraw Hill Professional, 2010.

[31] “Information Security information, news and tips - SearchSecurity.” https://searchsecurity.techtarget.com/

[32] “Information Technology Research & IT Advisory Company | Info-Tech Research Group.” https://www.infotech.com/

[33] “How to define SIEM strategy, management and success in the enterprise,” *SearchSecurity*. https://searchsecurity.techtarget.com/essentialguide/How-to-define-SIEM-strategy-management-and-success-in-the-enterprise

[34] Info-Tech Research Group, “Vendor Landscape: Security Information & Event Management, Optimize IT security management and simplify compliance with SIEM tools. Technical Report,” 2015.

[35] Solutions Review, “2020 Security Information and Event Management Vendor Map.” [Online]. Available: https://solutionsreview.com/security-information-event-management/security-information-event-management-vendor-map/.

[36] Splunk, “7 SIEM trends to Watch in 2019.” [Online]. Available: http://www.locuz.com/in/wp-content/uploads/2018/01/7-siem-trends-to-watch-in-2019.pdf.

[37] “DiSIEM Project deliverable D2.1. In-depth analysis of SIEMs extensibility,” 2017.

[38] Infosecnirvana, “SIEM Product Comparison - 2016.” [Online]. Available: http://infosecnirvana.com/siem-product-comparison-201/.

[39] C. Elliott, “GENI: Exploring Networks of the Future,” p. 39.

[40] “Federated cyber ranges.” https://federatedcyberranges.eu/

[41] “EDA Cyber Ranges Federation project showcased at demo exercise in Finland.” https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland

[42] “Cyber Range – Merit.” https://www.merit.edu/cyberrange/

[43] “Regent University Launches State-of-the-Art Cyber Range Training Center with Cyberbit,” *Regent University*, Oct. 03, 2017. https://www.regent.edu/news-events/regent-university-launches-state-art-cyber-range-training-center-cyberbit/

[44] “Arkansas Cyber Range | NICERC.” https://nicerc.org/arcybersecurity/

[45] “Cyber Range Hub - Educational Outreach - Wayne State University,” Jan. 08, 2020. https://wayne.edu/educationaloutreach/cyber-range/

[46] “Home,” *Florida Cyber Range*. https://floridacyberrange.org/

[47] “Virginia Cyber Range.” https://www.virginiacyberrange.org

[48] “DARPA - NationalCyberRange_FactSheet.pdf.” [Online]. Available: https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf.

[49] “20190208_1902-factsheet-cyber-defence-en.pdf.” [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

[50] “CRATE - Cyber Range And Training Environment.” https://www.foi.se/en/foi/resources/crate---cyber-range-and-training-environment.html

[51] “CHIPS Articles: DoD Cyber Range.” https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4035

[52] H. Holm, M. Karresand, A. Vidström, and E. Westring, “A Survey of Industrial Control System Testbeds,” in *Secure IT Systems*, Cham, 2015, pp. 11–26, doi: 10.1007/978-3-319-26502-5_2.

[53] J. Vykopal, R. Oslejsek, P. Čeleda, M. Vizváry, and D. Tovarnák, “KYPO Cyber Range: Design and Use Cases,” in *ICSOFT*, 2017, doi: 10.5220/0006428203100321.

[54] U. D. Ani, J. M. Watson, B. Green, B. Craggs, and J. Nurse, “Design Considerations for Building Credible Security Testbeds: A Systematic Study of Industrial Control System Use Cases,” *arXiv:1911.01471 [cs]*, Nov. 2019, [Online]. Available: http://arxiv.org/abs/1911.01471.

[55] E. C. Chaskos, “Cyber-security training: A comparative analysis of cyber- ranges and emerging trends,” p. 78, 2019.

[56] M. Xu, K. M. Schweitzer, R. M. Bateman, and S. Xu, “Modeling and Predicting Cyber Hacking Breaches,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2856–2871, Nov. 2018, doi: 10.1109/TIFS.2018.2834227.

[57] “Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks,” *Infosecurity Magazine*. https://www.infosecurity-magazine.com:443/white-papers/advanced-targeted-attacks-how-to-protect-against-t/

[58] “Cyber Ranges 101 and how they improve security training | Circadence.” https://www.circadence.com/blog/cyber-ranges-101-and-how-they-improve-security-training/

[59] “Cyber Security - GECI International - GECI International.” http://www.geci.net/Activity/13

[60] T. Grance, S. Chevalier, K. K. Scarfone, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” Sep. 2006, [Online]. Available: https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response.

[61] “Introduction to Digital Forensics | Virginia Cyber Range.” https://www.virginiacyberrange.org/courseware/introduction-digital-forensics

[62] “Digital Forensics – Cyber Warfare Range.” https://www.azcwr.org/about-us/areas-of-focus/digital-forensics/

[63] “Cyber range – JYVSECTEC.” https://jyvsectec.fi/cyber-range/

[64] T. Debatty and W. Mees, “Building a Cyber Range for training CyberDefense Situation Awareness,” in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2019, pp. 1–6, doi: 10.1109/ICMCIS.2019.8842802.

[65] “BlackHat-DC-2010-Powell-Cyber-Effects-Prediction-slides.pdf.” [Online]. Available: https://www.blackhat.com/presentations/bh-dc-10/Powell_Shane/BlackHat-DC-2010-Powell-Cyber-Effects-Prediction-slides.pdf.

[66] “CYBERWISER.eu | Cyber Range & Capacity Building in Cybersecurity.” https://www.cyberwiser.eu/

[67] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From game design elements to gamefulness: defining ‘gamification,’” in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, Tampere, Finland, Sep. 2011, pp. 9–15, doi: 10.1145/2181037.2181040.

[68] S. Scholefield and L. A. Shepherd, “Gamification Techniques for Raising Cyber Security Awareness,” in *HCI for Cybersecurity, Privacy and Trust*, Cham, 2019, pp. 191–203, doi: 10.1007/978-3-030-22351-9_13.

[69] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, “A Review of Using Gaming Technology for Cyber-Security Awareness,” 2016, doi: 10.20533/ijisr.2042.4639.2016.0076.