NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATION

INTERPARTMENTAL GRADUATE PROGRAM IN
MANAGEMENT AND ECONOMICS OF TELECOMUNICATION NETWORKS

MSc THESIS

Cyber-security training: A comparative analysis of cyber-ranges and emerging trends

Evangelos C. Chaskos

Supervisor: **Nicholas E. Kolokotronis,** Associate professor

ATHENS

MARCH 2019

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εκπαίδευση για την ασφάλεια στον κυβερνοχώρο: Συγκριτική ανάλυση των *cyber range* και των αναδυόμενων τάσεων

Ευάγγελος Χ. Χάσκος

Επιβλέπων **Νικόλαος Κολοκοτρώνης,** Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΜΑΡΤΙΟΣ 2019

MSc THESIS

Cyber-security training: A comparative analysis of cyber-ranges and emerging trends

Evangelos C. Chaskos
SN.: MOP509

Supervisor: **Nicholas E. Kolokotronis,** Associate professor

MARCH 2019

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εκπαίδευση για την ασφάλεια στον κυβερνοχώρο: Συγκριτική ανάλυση των *cyber range* και των αναδυόμενων τάσεων

Ευάγγελος Χ. Χάσκος
Α.Μ.: ΜΟΠ509

Επιβλέπων **Νικόλαος Κολοκοτρώνης,** Αναπληρωτής Καθηγητής

ΜΑΡΤΙΟΣ 2019

ABSTRACT

Cyber-attacks are becoming stealthier and more sophisticated can stem from various sources, using multiple vectors and taking different forms. The need for building and experimenting on advanced cyber-security mechanisms, as well as continuous training using state-of-the-art methodologies, techniques and up-to-date realistic scenarios is vital. *Cyber Ranges* can provide the environment where cyber-security experts and professionals can practice technical and soft skills and be trained on emulated large-scale complex networks in the way to respond to real-world cyber-attack scenarios. Furthermore, they can simulate an environment for information security professionals, to evaluate incident handling and response procedures and to test new technologies, in order to help prevent cyber-attacks. The main objective of this paper is to describe the functionalities of various Cyber Ranges and to highlight their key components and characteristics, to demonstrate a high-level architecture of a state-of-the-art Cyber Range while classifying the features of the reviewed Cyber Ranges according to the attributes of the proposed one.

SUBJECT AREA: Cyber Range

KEYWORDS: Cyber-threats, cyber-security, simulation platforms, risk analysis, threat forecasting.

ΠΕΡΙΛΗΨΗ

Οι επιθέσεις στον κυβερνοχώρο γίνονται όλο και πιο προηγμένες και δύσκολα ανιχνεύσιμες, προέρχονται από ποικίλες πήγες και πραγματοποιούνται λαμβάνοντας πολλαπλές διαστάσεις και παίρνοντας διάφορες μορφές. Η ανάγκη οικοδόμησης και πειραματισμού σε προηγμένους μηχανισμούς ασφάλειας στον κυβερνοχώρο, καθώς και η συνεχής κατάρτιση με τη χρήση σύγχρονων μεθοδολογιών, τεχνικών και ενημερωμένων ρεαλιστικών σεναρίων είναι ζωτικής σημασίας. Τα *Cyber Ranges* μπορούν να προσφέρουν το περιβάλλον μέσα στο οποίο οι ιδικοί και επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο μπορούν να εφαρμόσουν τεχνικές και δεξιότητες και να εκπαιδεύονται σε προσομοιώσεις σύνθετων δικτύων μεγάλης κλίμακας, προκειμένου να ανταποκριθούν σε πραγματικά σενάρια επίθεσης στον κυβερνοχώρο. Επιπλέον, μπορούν να προσομοιώσουν ένα περιβάλλον για τους επαγγελματίες της ασφάλειας πληροφοριών, να αξιολογήσουν τις διαδικασίες χειρισμού και αντιμετώπισης περιστατικών και να δοκιμάσουν νέες τεχνολογίες, προκειμένου να βοηθήσουν στην πρόληψη επιθέσεων στον κυβερνοχώρο. Κύριος σκοπός της παρούσας εργασίας είναι να περιγράψει τις λειτουργίες διαφόρων *Cyber Ranges* και να τονίσει τα κύρια δομικά στοιχεία και γνωρίσματα τους, να παρουσιάσει την υψηλού επιπέδου αρχιτεκτονική ενός υπερσύγχρονου *Cyber Range* και ταυτόχρονα να ταξινομήσει τα χαρακτηριστικά των υπό ανάλυση *Cyber Ranges* σύμφωνα με τα χαρακτηριστικά του προτεινόμενου.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: *Cyber Range*

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Απειλές στον κυβερνοχώρο, ασφάλεια στον κυβερνοχώρο, πλατφόρμες προσομοίωσης, ανάλυση κινδύνου, πρόβλεψη απειλών.

AKNOWLEDGMENTS

The present thesis is a result of hard work, perseverance, in-depth study and commitment to the science of Informatics. I consider myself very fortunate that many people contributed to my work and helped me along the way. It has been a unique experience.

First and foremost, I would like to express my sincere gratitude and appreciation to my supervisor Mr. Kolokotronis, Associate professor of the department of Informatics and Telecommunication at University of Peloponnese, for all the guidance and support. His valuable advices, suggestions, insightful feedback and patience kept me focused and made me strive for the best. I am indebted to him for imparting his knowledge, for always being willing to help me and for giving me complete freedom.

In the challenging process of writing this thesis, I am thankful to all my friends and colleagues, who have supported me. I' m grateful for their encouragement, the fruitful discussions, but above all for their friendship and all that we shared during hard times. I owe so much to them for helping me take my mind off my work when I needed it the most and for all the beautiful moments that helped me stay positive.

Finally, I am more than grateful to my family and my partner for always being by my side during tough times. It would have been impossible without their emotional support, continuous encouragement and constant presence, that helped me overcome all the difficulties I was facing. Their belief in me has always been the biggest motivation. A special thanks goes to my father, who, even while not being present has been the most powerful source of inspiration.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Cyber-attacks occur worldwide on a daily basis; information and communication systems as well as the *critical information infrastructures* (CIIs) are exposed to them. Those attacks are increasing in both sophistication and scale. *Critical information infrastructures* provide vital functions that our societies depend upon, they are expected to have a significant negative economic and societal impact in the next decade and should be considered as global risks. A review report recently published by the European Union Agency for Network and Information Security (ENISA) estimates that the average annual losses due to cybercrime among *European Union* (EU) countries is 0.41% of their *gross domestic product* (GDP); in some countries (Germany and the Netherlands), the losses exceed 1.50% of the GDP, leading to annual costs in the range of €425K – €20M per company. Amongst the CII sectors in the EU, the significantly affected ones seem to be energy, finance, health, transport, *information and communication technology* (ICT) and public administration.

The aforementioned economic losses from cybercriminal activities are exceeding the security investments made by companies worldwide in information technology (IT) in order to protect their assets. This situation is facilitated by the technological evolution brought by the *Internet of Things* (IoT), which establishes new ecosystems of networked heterogeneous devices that are highly complex to analyze, maintain and secure. As a result, there has been a rapid growth of new types of cyber-attacks that are becoming stealthier and more sophisticated. New vulnerabilities appear constantly and cyber-threats evolve very quickly to take advantage of them. Traditional vectors of attack, such as spam and adware, which were considered as major threats just a few years ago, are rapidly being replaced by more complex threats. These include sophisticated denial-of-service attacks (DoS attacks) or ransomware, i.e. a type of malicious software designed to block access to a computer system to extort or blackmail the victim. There are many recent examples where (highly insecure) Internet appliances have been exploited, so as to hijack communication links, spy on people and steal personal data, or even to perform network attacks of unprecedented scales. A small selection of incidence that took place [1]:

- November 2016, NHS hospitals: Hospital machines were frozen to demand ransom cash; at least four NHS (National Health Service) funds were attacked.
- November 2016, Yahoo: Data breach of 1 billion accounts.
- December 2015 & December 2016, Power grid in Ukraine: 230,000 people were left without power for up to 6 hours; first time that a cyber-weapon was successfully used against a nation's power grid.
- February 2016, Central bank of Bangladesh: 81 million USD was lost and a further of 850 million USD in transactions was prevented from being processed.
- October 2016, Australian Red Cross: Personal data of 550,000 blood donators stolen.

- November 2016, Deutsche Telekom: 900,000 (or about 4.5 percent of its 20 million fixed-line customers) suffered Internet outages over two days.

In many cases, there are early signs of the emerging cyber-threats (e.g. the WannaCry ransomware campaign, the Mirai malware etc.), but due to the security technology market fragmentation in cyber-defence systems, the security skill shortage and the lack of security executives' deep awareness of cyber-security risks, the threats could not be accurately forecasted, and thus people were unprepared to properly deal with them. This fact, when combined with the low adoption of cyber-insurance practices, makes it quite hard for companies and other organizations to understand and effectively manage such risks [2]. The above presents the need for building and experimenting on advanced cyber-security mechanisms, as well as continuous training using state-of-the-art methodologies, techniques and up-to-date realistic scenarios. Attacks can stem from various sources, using multiple vectors and taking different forms.

2. CYBER-SECURITY EDUCATION AND TRAINING

Cyber-security education and training are becoming more and more relevant, as they are the only way to prevent and adequately handle such cyber-breaches. As the importance of securing computer systems grows, so does the cyber-security workforce shortage. It is expected that by 2022, 1.8 million positions that require cyber-security expertise will be unfilled, stressing the importance of educating security professionals [3]. More skilled cyber-security professionals are needed, because the number of cyber-threats and attackers' ingenuity are ever growing [4]. With respect to cyber-security, we are now facing an emergency, because sufficient talented specialists that the industry is frantically looking for have not been created, and stakeholders moreover need information to understand the nature of cyber-space.

A "constructive change of higher education" is critically required, but it has to quickly respond to such needs for high growth. It is imperative that the synergies between higher education and proficient training do not compete, but are reinforced. To satisfy the developing request for talented cyber-security experts, instructive openings have to be extended at all levels, the number of qualified teachers should increase, synergies between instructive ways and preparing conceivable outcomes in a working environment should be created, the gifted specialists should be reached, and the basics of deep learning in cyber-security should be established. Also, to address the above problems, new teaching and knowledge transfer methods that evolve like Cyber ranges (CR) and technical exercises must be applied [5]. Scalable and professional training, with a more individual and academic approach involving deep learning of the basic concept through the range of high-complexity sections. Integration of research must be applied between the cooperative organizations.

The cyber-security teaching domain should not only refer to IT, but it should be implemented as a holistic approach. Cyber-security related training, education and certifications shall be comparable and also the gained knowledge shall be validated. Eventually, cyber-security instruction must begin at school, to induce young individuals fascinated by innovation, IT and cyber-security subjects. Cyber-education is a learning process focused on the synthesis of knowledge and skills, and the applicability of these skills in solving complex issues. Knowledge and skills required for cyber-defence can be developed and exercised through lectures and lab sessions, or through active learning, which is considered as a promising and attractive alternative. Cyber-security can be taught not only using conventional methods, including classroom lectures, seminars or home assignments, but also through hands-on experience [6]. In recent years, there has been a significant growth of hands-on competitions, challenges and exercises. It is believed that these enable participants to effectively gain or practise diverse cyber-security skills in an attractive way. The purpose of training through hands-on competitions, challenges and exercises using simulated environments is to analyse the possible impact on confidential data, the decision-making process, but also on how the personnel involved responds to the arising critical situation [7]. Hands-on lab training can be achieved through various ways: general test beds, which are usually virtual machines

(VMs) that can simulate various network features; lightweight platforms, which are usually web-based platforms and offer practical exercises; and Cyber Range Infrastructures [8].

3. CYBER RANGE

A *Cyber Range* is the environment where cyber-security experts and professionals can practice technical and soft skills and be trained on emulated large-scale complex networks in the way to respond to real-world cyber-attack scenarios under specific (and general) domains. CR is usually an isolated virtual training environment designed for cyber-security training, operational support and project support; it contains the entire required infrastructure, so that trainees can experience and participate in real-world simulated cyber-attack or defense scenarios. The more realistic the simulated scenario the more prepared the trainees will be to face real-world attacks. It is also used for cyber-warfare training and cyber-technology research and development. It provides tools that help strengthen the stability, security and performance of cyber-infrastructures. The platform includes endpoint prevention, detection and response, operation technology security and attack simulations.

More specifically, a Cyber Range is a simulation platform created for information security professionals, to evaluate incident handling and response procedures and to test new technologies, in order to help prevent attacks. A cyberspace recreates the experience of responding to a cyber-attack, copying the security operations center (SOC) environment, the organizational network and the attack itself. As a result of this process, practical training is provided in a controlled and secure environment. The more realistic the whole simulation the better the cyber-construct series that can properly prepare trainees to better and more realistically respond to all incidents of random attacks. Thus, the probability of malicious intrusion in our systems is reduced. Cyber Range is a robust training platform which allows the simplification of analyst training with quick and effective training for the experts, which can evaluate processes and procedures and provide an effective test bed.

Besides skill development, such systems also allow for a holistic approach to cyber-threat management by providing the means to test the effectiveness of a CII's security framework. Typically, CR systems provide a number of functionalities, including [9]:

» *Project support:* product evaluation, testing fitness for purpose; specific capability development; benchmarking testing.

» *Operational support:* skill development and training for cyber-operations; war-gaming or *capture the flag* (CTF) exercises and cyber-competitions; counter-cyber-warfare.

» *Research and development:* research on advanced cyber-threats; experimentation; novel ideas development; tools development.

Cyber-competitions play a central role in CR systems and can be designed so as to support different scenarios, where offensive (red) and defensive (blue) teams try to attack and protect assets in an infrastructure or computer network respectively, as well as solve cyber-related challenges.

» *Technical competitions*, i.e. CTF exercises, can take the form of offensive-defensive activity on a network or that of jeopardy-type questions [10].

The former allows the competing players to simultaneously or sequentially choose a strategy for defending their own or infiltrating the opponent's network and achieving their goals, whereas the latter involves answering questions on various cyber-security topics, like forensics [11], cryptography etc.

» *Operational competitions* aim at evaluating teams in various business challenges that are related to a security professional's job function.

CR systems have been developed for a number of specialized stakeholders: (a) defense organizations, (b) *computer emergency response teams* (CERTs) and computer security incident response teams (CSIRT), and (c) network operations center (NOC)/SOC teams of large service providers and mission-critical control systems. The US national CR [12], which was established by the *defense advanced research projects agency* (DARPA), is amongst the most well-known CRs; it constitutes a platform for cyber-security testing using unique methods to assess the resiliency to advanced cyber-threats. Recently, DARPA has also launched the *cyber grand challenge* (CGC), a competition for the development of *cyber-reasoning systems* capable of automatically identifying software flaws, as well as issuing and deploying patches in real time. Along the same direction, the main idea of the proposal is to explore the potential of artificial intelligence (machine learning, deep learning etc.) and other related areas to build a sophisticated Cyber Range platform that allows playing games with intelligent attackers or defenders.

3.1 Related work

Nowadays, due to the continuous growth of the critical information infrastructures accompanied by the evolution brought by the Internet of Things, advanced cyber-security education and awareness is deemed necessary. Cyber Ranges can provide the required advanced training and education on emulated large-scale complex networks. Only a handful of works in literature describe the characteristics of the existing Cyber Ranges and classify them according to their characteristics. The Australian Department of Defense has published a survey of cyber ranges and test beds (Davis and Magrath, 2013),[9] which describes their purpose and functionality. Solms and Peach in their research [13] focus more on node emulation in a network simulation platform in two Cyber Ranges. In other papers, Pastor, Diaz and Castro [14] describe simulated system platforms as to information security and information assurance education, training and awareness. Vykopal, Vizvary, Oslejken, Celeda and Tovarnak describe mainly the KYPO Cyber Range [15] and define the deferent learning environments, such as (i) Generic test beds (ii) Lightweight platforms (iii) Cyber Ranges [16]. The main contribution and objective of this paper is to describe the functionalities of various Cyber Ranges and to highlight their key components and characteristics with the available resources found in open literature. Additionally, in this paper, a high-level architecture and features of a state-of-the-art Cyber Range will be demonstrated, while classifying the features of the reviewed Cyber Ranges according to the attributes of the proposed one.

4. REVIEW OF CYBER RANGE PLATFORMS

Reviewing the existing CR platforms, various approaches have been taken for their development. The construction of a CR depends on the approach to design features such as flexibility, scalability, isolation, interoperability, effectiveness, access, service-based access, scoring and evaluation, and risk evaluation. They can also be categorized by their supporting sector: academic, military or commercial; and furthermore, they can be categorized by the capabilities which they support. In this section, sixteen CR environments will be demonstrated, and their mission, capabilities and advantages will be highlighted. At the end of this section, a summary of their features is presented.

4.1 KYPO Cyber Range

The KYPO project was funded by the Ministry of Interior of the Czech Republic as part of the Security Research Program of the Czech Republic. To be able to create real-world scenarios, KYPO is designed as a modular distributed system. Its modular architecture is run on various computation platforms, such as OpenStack or OpenNebula. This allows it to be flexible and scalable to the creation of the virtual scenarios. The high-level architectural design is based on the following requirements: (i) Flexibility (ii) Scalability (iii) Isolation vs. Interoperability (iv) Cost-effectiveness (v) Built-In Monitoring (vi) Easy Access (vii) Service-Based Access (viii) Open Source. With the above requirements, real-world simulated scenarios can be created in a dynamic way. The scenarios' complexity is in the range of creating a single isolated instance (a Node) to an isolated multiple-connection network with various network topologies and operating systems. This enhances the flexibility of the platform and the scalability of the scenario creation of the platform. Cost-effectiveness in combination with Scalability drive the decisions to use cloud-based Sandboxes for the training exercises. With Service-Based access, KYPO offers the platform as a service. The platform is accessible through web-interface; therefore it achieves easy access for the more inexperienced users. The platform can provide real-time and historical data for monitoring the overall interoperability of the platform and the individual topologies that the platform can create. To be able to achieve all the above requirements and features, the platform is divided in the following building blocks: (i) The computing infrastructure includes datacenter facilities, physical machines and network devices, which form the computing resources of the infrastructure (storage – processing power – operating memory). (ii) To manage the above computing resources, OpenNebula platform is used and provides the Data Center Virtualization management as well as the cloud management. (iii) The monitoring API as described above has the functionality of monitoring the network topologies, the hosts and all the components of the infrastructure, combined with the cloud API that translates OpenNebula commands to common API methods. (iv) The scenario and sandbox management APIs are used to manage the various sandboxes. (v) The Portal is the interface where the users can interact with the created sandboxes. These components interact, in order to build and manage sandboxes in the underlying cloud computing infrastructure. The KYPO platform can provide from a single sandbox, where, for example, researchers can do malware

analysis, to a real-life network topology, where various teams can compete to capture the flag exercises.

Table 1: KYPO Cyber Rang Mission - Capabilities - Advantages

Cyber Range	Mission	Capabilities	Advantages
KYPO CR	Realistic environment for cyber-training and support for cyber-testing, research, and training for students and researchers.	Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks can be replicate for multiple and simultaneous usage	Complete training stack, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification, Capture-the-flag environment

4.2 Department of Defense Cyber Security Range

The Department of Defense (DoD) Cyber Security Range (CSR) is funded by the 2009 Comprehensive National Cyber Security Initiative (CNCI) and is located near Marine Corps Base, Quantico, in Stafford, VA. The DoD Cyber Security Range has supported missions for the US Marine Corps, US Army, US Navy, US Air Force, National Security Agency (NSA) and the Office of the Secretary of Defense (OSD) as well as other organizations. It provides an environment that supports training and educational exercises with real-world network simulations. The infrastructure of the DoD CR is a virtualized environment running on VMware vSphere version 5.1 and VMware vCenter. There are over 3,000 virtual machine profiles to support provisioning of the virtual machines. To reduce power consumption and back up the virtual machines, the Tintri VMstore T540 and T650 are used, three networks of storage with corresponding backup arrays. The virtualized environment handles all the hardware resources. The architecture is based on three principals:

- Resource Authoring, which is the resource object for the virtualization
- Event Authoring graphical drag and drop topology configuration
- Event Orchestration, which is the automated management for all the cyber-range virtual resources

DoD CR uses the Joint Regional Security Stack (JRSS), which is the suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding (VRF), and which provides a host of network

security capabilities. It is a virtual environment with no cloud capabilities for the creation of sandboxes. The upper layer includes the hardware along with the orchestration engine. In the lower layer, Virtual Desktops Interfaces are created connected to multi-vendor security applications.

Table 2: Department of Defense Cyber Rang Mission - Capabilities - Advantages

Cyber Range	Mission	Capabilities	Advantages
DoD Cyber Security Range	Environment to support exercises, training, testing, evaluation, and education for the military.	Traffic generator, configurable user emulation, malware, spyware, and botnets emulation	Cyber-security and computer network defence

4.3 National Cyber Range

The National Cyber Range (NCR), operated by the Test Resource Management Center (TRMC), provides the ability to produce realistic cyber-security testing, evaluation and training. The architecture is the same as the KYPO cyber range. A common resource pool of hardware is used to create a virtual environment where the Cyber Range management Portal will create isolated secure test beds. There are also encapsulation tools for the automation and monitoring as well as automation toolkits for the simulations.

The four main components of the NCR are:

A secure facility: Where the operator rooms, the range, the operation center, the range support center and of course the data center of the infrastructure are
A network encapsulation architecture and operational procedure:

- Common pool of hardware and software resources
- Utilization of test specification tools to define end-to-end aspects of the tests.
- Automated allocation of the appropriate resources.
- Configuration tools for automated hardware configuration.
- Configuration tools for automated software configuration.
- Running of the created test and collection of the data for monitoring and evaluation.
- Release of the allocated resources back to the hardware pools for later usage.

An integrated Software Testing Tool Suite: For the automation of the creation of faster and more reliable environments following the above procedure. Here, the Test Scientist will create the test specifications, where the operation team will manage the required resources, so that the test bed can be created and the participants can participate to the specific test. Sensors, traffic generation tools, data analysis and visualization tools are used to accomplish the specifications of the test bed. The test management verification control and the event execution language are used to automatically build, verify and sanitize the environment.

Cyber Test Team: The cyber test team provides end-to-end test support for the design face as well as the execution face. They also provide thread vector development custom traffic generation data analysis and support for the hardware and software, as well as support to the various games the platform can create (e.g. Red / Blue team)

Table 3: National Cyber Range Mission - Capabilities - Advantages

Cyber Range	Mission	Capabilities	Advantages
US Nat'l CR	Realistic environment for cyber-training and support for cyber-testing complex governmental systems.	Secure facility, role-based access, focus in cyber-security and computer network defence	Malware analysis, forensic analysis, architecture analysis, training events, research, Capture-the-flag environment, testing and product evaluation

4.4 Virginia Cyber Range

The Virginia Cyber Range's scope is to enhance cyber-security education for students in Virginia's high schools and colleges. The Virginia Cyber Range seeks to increase the number and the preparedness of students entering the cyber-security workforce in operations, development and research. It is cloud-based and provides sandboxes to the trainees and a big variety of security exercises in a virtual isolated environment. One of the key design considerations that have been made to achieve flexibility and scalability is to be hosted in the cloud. It provides user-specific content as well as role-based access to the platform. To achieve cost reduction and better resource allocation of the infrastructure, the created virtual environment is dynamically created and destroyed. Furthermore, large target networks can be replicated for multiple and simultaneous usage providing large-scale exercises and capturing the flag environments [17].

Table 4: Virginia Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Virginia CR	Provide an environment to increase the number, and the preparedness, of students entering	Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks	Cyber-security and computer network defence, training exercises for SCADA and ICS, cyber-law and

	the cybersecurity workforce in operations	can be replicate for multiple and simultaneous usage	policy topics, CTF competitions

4.5 CYBERBIT Cyber Range

Cyberbit is a provider of cyber range environments which aims to provide hyper-realistic simulated training environments to enterprises, governments, academic institutions and managed security service providers (MSSPs) around the globe. Cyberbit Range is a simulation platform for training participants in cyber-security topics [18]. It delivers realistic training scenarios and provides test beds for assessing security tools and architectures in a safe and controlled environment. Cyberbit CR can provide virtual replicas of enterprise IT and operational technology (OT) networks that include application servers, database servers, email servers, switches, routers and programmable logic controllers (PLCs), which can achieve real-life attack and defence scenarios in a hyper-realistic network environment. It can emulate complex networks and also provide training content of industrial control system (ICS) for critical infrastructure organizations. Virtual machines as well as additional appliances are used for the simulated network, traffic and threats. Physical OT hardware can be integrated to the simulated IT and supervisory control and data acquisition (SCADA) environment. A customized traffic generator and an attack simulation are also supported in the created scenarios. It also supports real-time monitoring of the training session as well as score and evaluation of the training [19]. Cyberbit as a provider of Cyber Range environments has collaborated with Regent University, Miami, Dade College, Telekom Austria, Maryland Range and CloudRange.

Table 5: Cyberbit Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Cyberbit CR	To provide hyper-realistic simulated training environments to enterprises, governments, academic institutions and MSSPs.	Virtual Network Replica, Attack Generator, local and remote seats for trainees, Pre-Build Networks, User Generated Networks, Pre-Build Scenarios, User generated Scenarios, inject real-life attack scenarios to the network, Realistic Traffic Generator, Knowledge base, real time monitoring, score and evaluation, Virtual and physical SCADA training, cross-functional executive training and new attack scenarios such as ransomware variants.	Complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing and IR, certification courses, Capture-the-flag environment.

4.6 Raytheon Cyber Range

Raytheon is an international aerospace and defence company specialized in various sectors, such as defense, civil government and cyber-security solutions. Raytheon Cyber develops and distributes cyber-security products and solutions to its clients. Raytheon cyber range helps their customers to test the resilience of critical technologies. It provides a versatile environment to create realistic training exercises. It can provide predefined network topologies or, with the cooperation of Raytheon Cyber Operations, Development and Evaluation (CODE) Centre, exact replicas of the customers' network including critical infrastructures network, such as Air Traffic Control, Power Grids, Water Supplies or Security Operations Centres. Raytheon CR has a scalable and agile architecture that enables the emulation of complex enterprise networks up to internet scale, and it provides automated tools for the creation and destruction of the network topologies. Raytheon CR is an isolated environment, but it can interconnect with external hardware resources for carrying out cooperative testing on a larger scale.

Table 6: Cyberbit Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Raytheon CR	To provide an environment to support training and education for companies.	Network environment emulation for air traffic control, power grids, water supplies, SOCS capabilities, scalable and agile architecture, automation, interconnection with external hardware.	Reverse engineering, firmware code analysis, Radio frequency and wireless vulnerability and radiated emissions testing, cyber professional training, penetration testing, Mitigation planning and consulting, Capture-the-flag environment.

4.7 CISCO Cyber Range

The Cisco Cyber Range is offered as a service. It is a training course that aims to train the participants to combat modern cyber-threats. Cisco CR is based on real-world scenarios and provides a war-gaming environment that allows participants to play the role of both the attacker and the defender, in order to learn the latest methods of vulnerability exploitation, and the use of advanced tools and techniques to mitigate the threats. The Cisco CR provides real-life experience of reacting to and defending against complex cyber-attacks, including advanced persistent threats (APTs). It provides training in security methodologies, operations and procedures using a variety of security tools and techniques. Cisco CR is a cloud-hosted environment that simulates the network and

applications of a typical enterprise customer, which can be accessed remotely. It simulates more than 50 different attack scenarios and more than 100 real applications and it is equipped with visibility-based and platform-based security tools. Cisco CR provides the foundation of a cyber-security course as well as mitigation methods using Cisco's products, such as Splunk, Stealthwatch, TrustSec, firewalls and IDS. It can be combined with other Cisco courses in the security domain, such as securing networks with firewalls, and intrusion detection system [21].

Table 7:Cisco Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Cisco CR	To provide an environment to support training and education for the participants of an organization to combat modern cyber-threats.	Implemented with variety of application which provide visibility, intelligence, threat detection, firewalling and thread detection e.g. Cisco Stealthwatch, Cisco Splunk, Control. Includes traffic generator, configurable user emulation, malware, spyware, and botnets emulation, individual and team training, end-to-end real-time solution for machine data delivery.	Focus in cyber-security and computer network defense, threat detection, identification of various application, network traffic pattern, secure network and applications, Cisco Stealthwatch, Cisco Splunk, Cisco TrustSec.

4.8 European Space Agency Cyber Range

The European Space Agency (ESA) Cyber Range aims to deliver a training and simulation platform facility to provide training and testing and to develop knowledge in awareness, detection, investigation, response and forensics, in order to counter cyber-attacks specific to the space sector. The ESA Cyber Range provides a virtualization environment in which relevant space systems and missions can be simulated to provide a realistic environment for the hosting of cyber-security-related training courses. The virtual environment supports the instantiation of a full mission environment, mission control systems, pre-launch environment procedures, launch environments, ground and satellite simulators [22].

Table 8:European Space Agency Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
ESA CR	To provide a training and simulation platform facility to provide training and testing and develop knowledge in awareness, detection, investigation, response and forensics to counter cyber-attacks specific to the space sector	Provide specialized space cyber-emulation environment to securing space assets	Instantiation of a full mission environment, mission control systems, Pre-Launch, Launch, LEOP, IOT, ground and satellite simulators, space segment, data segments, operations and development networks

4.9 CybExer Cyber Range

CybExer Technologies OÜ is a joint company established by two Estonian cyber-security and cyber-solutions companies: BHC Laboratory OÜ and Bytelife Solutions OÜ. CybExer Range Platform can be deployed on-premise in an organization or it can be accessed through CyberExer infrastructure, and it provides complex technical cyber-security exercises in various cyber-security domains. It also provides a Capture-the-flag environment. The CybExer CR provides an automated way for the creation and destruction of virtual environments; it has features for the creation of custom scenarios and a gamenet module for the creation of cyber-security exercises. Moreover, it can be integrated to a cyber-hygiene module, which provides an interactive tool for human risk-behaviour mitigation in cyber-security with an integrated e-Learning Platform and a Risk Evaluation Tool that aims to address human risk behaviour in cyberspace. Its goal is to identify specific risk areas in which the participant may be affected. The specific tools provide an understanding of human risk behaviour within the organisation. Finally, it supports an Integrated Scoring and Awareness module, for which it provides a sophisticated and precise data visualisation framework [23].

Table 9: CybExer Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
CybExer CR	Environment to support training and education for	Exercise management, red teaming capability, exercise Management Toolkit, automation, customized scenarios,	Complete training stack, trainer console, training scenarios,

	companies and military.	GAMENET, Cyber Hygiene, Integrated Scoring and Awareness	advanced customization tools, malware forensics, network security, penetration testing, certification, Capture-the-flag environment

4.10 IBM Cyber Range

IBM Cyber Range aims to offer the experience of a cyber-attack at IBM X-Force Command Center. It aims to train all the departments of an enterprise, from SOC to human resources (HR) and Legal. It offers Blue vs Red team training in a variety of security attack vectors and it helps the organization to develop a response plan in a holistic approach (not only the security teams). The goal is to give participants the feeling and the responsibility they must have in an attack as realistically as possible, so that the participant will be able to be better prepared to face events in their production networks. IMB CR is the only one that focuses on the plans and the procedure of an organization in a cyber-incident. Furthermore, it provides Cyber wargame training aiming to improve the collaboration between the engaged teams [24].

Table 10: IBM Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
IBM CR	Provide an environment to offer an experience in a cyber-incident	Exercise rapid-response thinking in a pressured environment, understand how security solutions work together, experience how your teams work together.	Discover gaps in enterprise's response plan, technical cyber response and leadership best practices, attacking tools, cybercrime topics, risk analysis

4.11 Palo Alto Networks Cyber Range

Palo Alto Networks Cyber Range [25] is headquartered in Amsterdam with hubs is Washington DC, Santa Clara and Sydney. Palo Alto Networks CR is offered as a service to organizations, but it can also be implemented on-premise in an organization data center. It is based on network simulations and attack – defense exercises, which aim at identifying the cyber-threats using an innovative technology in hands-on exercises. The training scenarios are hyper- realistic as they are related to real threats. They are powered by the Cyber Test System using network traffic generators that are able to generate up

to 400 Gbps of legitimate and malicious traffic, and an application traffic generator that generates up to 40 Gbps and can replicate users' behaviour. With the support of Cyber Test appliances, it can emulate Green, Red, Yellow and White teams in the created scenarios (the Blue team cannot include the trainees). The aim of the courses provided by Palo Alto CR is that trainees can master various defence techniques and skills, participate in a hyper-realistic isolated environment and experience a cyber-attack's lifecycle.

Table 11: Palo Alto Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Palo Alto CR	To train the participants of an organization to combat modern cyber-threats and enhance their prevention, detection and response skills through hyper-realistic network simulation exercises	Provides an isolated and realistic environment with network traffic-generator capabilities, application traffic-generator, multiple courses.	Identify advanced attacks, mitigate advanced attacks, collaboration between teams, Industrial Control Systems attack scenarios, various training scenarios, Capture-the-flag environment

4.12 Silensec Cyber Range

Silensec is an Information Security Management Consulting and Training company. Silensec Cyber Range provides an environment for individuals and organizations to practise cyber-security skills in a fun and challenging way [26]. The key design component of Silensec CR is based on gamification, advanced visualization and scenario plots. Trainees can compete in various exercises covering a wide variety of cyber-security domains. Silensec offers various training courses through the platform in protection, detection and reaction as well as preparation for certifications like CISSP. The infrastructure is built on cloud for better scalability and can be intergraded to IoT and Industrial Control System environments, while it offers competence-based scoring and assessment [27]. Silensec CR furthermore supports custom scenario generation with storylines, and cyber-challenges and can be offered as a service, hosted or on-premise.

Table 12: Silensec Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Silensec CR	To provide a training environment for individuals and enterprises to practice cyber-security skills in a fun and challenging way through advanced gamification modules.	Advanced monitoring, SIEM, cloud based, available as a service, support interconnection with IoT and ICS environments, competence-based scoring and assessment, virtualization automation.	Protection, detection, reaction, certifications, various training scenarios, indent response and investigations, Capture-the-flag environment and cyber-security competitions.

4.13 Austrian Institute of Technology Cyber Range

The Austrian Institute of Technology (AIT) [28] CR aims to share the knowledge in cyber-security with various actors, such as critical infrastructure providers, industry, research and public sector, providing an isolated and realistic environment for testing and analysing various scalable scenarios in the cyber-security domain. AIT CR training is based on security exercises and competitions with individual and team capabilities on different levels. AIT CR aims to enhance cyber-security awareness through the courses they offer, which is addressed not only to security officers but also to personnel on management level. AIT CR does not focus only on practical skills, but it also offers risk assessment and evaluation modules that enhance modern risk management. AIT CR provides a realistic environment that is enhanced with visualization modules, and a flexible architecture that can provide simulation of industrial control systems, digital networks and critical infrastructures, such as the International Atomic Energy Agency (IAEA).

Table 13: Austrian Institute of Technology Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
AIT CR	An environment for sharing the knowledge in cybersecurity domain for critical infrastructure providers, industry, research and public sector.	Advanced training exercises and competition on different levels, visualization, industrial control systems, digital networks and critical infrastructures, focus in cyber security research and development.	Various training scenarios, offers risk assessment and evaluation modules, certifications, testing of contingency plans, incident response processes.

4.14 IXIA Cyber Range

IXIA is a security assessment company focusing on the security and monitoring of networks. IXIA offers a variety of its products as a Cyber Range solution. IXIA CR offered as a service can replicate corporate networks and the created scenarios can be inserted with real malicious traffic like distributed denial-of-service (DDoS) attacks with the application and threat intelligence (ATI) service. It focuses on attack and defence exercises (blue and red team training), in a variety of attack – defence scenarios. IXIA's CR is designed by several combined modules from their portfolio and various other vendors, which makes its design stand out. Is uses Splunk's [29] analytics-driven security information and event management (SIEM), Quali [30] for the creation of the sandboxes and management interface, Fortinet next-generation firewalls [31], IXIA's ThreatARMOR for threat intelligence feeds, IXIA's PerfectStorm as a traffic generator up to a terabit of traffic, and IXIA's BreakingPoint for the visualization module [32]. The differentiation of its architectures with various modules makes it capable of interconnecting with external systems, which makes it versatile, flexible and scalable (interconnection with Palo Alto next-generation firewalls for the creation of a Blue – Red team simulating training environment).

Table 14: IXIA Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
IXIA CR	Provide an environment to train the participants of an organization to combat modern cyber-threats using a variety of IXIA's products	Offered as a service, flexible, scalable, application and threat intelligence, visualizations modules, SIEM, traffic generator	Complete training stack, trainer console, training scenarios, advanced customization tools, various training scenarios, Capture-the-flag environment and cyber-security competitions.

4.15 NEC Cyber Range

The NEC Cyber Range is offered as a service and aims to provide their customers with a virtualized framework for cyber-security training, modelling and simulation. NEC CR has three major components: (i) Virtual Training Platform (VTP), which orchestrates the knowledge base and injects cyber-security training exercises to its modules, (ii) Cyber Analytics and Simulation Platform, which is responsible for the customized virtual environments as well as the risk assessment modules, (iii) Sypris [33] Cyber Range,

which is responsible for the team-based cyber-security exercises and the simulation of various industrial control systems [34]. The virtual environments that can be created are scalable and able to simulate a multi-site industrial control system, such as SCADA.NEC CR provides an operationally-focused approach classifying the training modules according to the operational roles, providing a wide variety of training modules in a variety of skill levels. It supports a service-based access through a web interface and the VTP supports interconnection with the third-party applications and training contents, as well as with physical systems.

Table 15: NEC Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
NEC CR	To provide an environment to customers a virtualized framework for cyber-security training, modelling and simulation	Self-paced security challenges in various topic areas, classroom-based training for different levels of expertise, team-based exercises, interconnects with physical systems.	Complete training stack through classroom module, training scenarios, network security, penetration testing, certification, Capture-the-flag environment.

4.16 Augusta University Cyber Range (Georgia Cyber Institute)

Georgia Cyber Range [35] is available to students, industry and government professionals and aims to strengthen cyber-security preparedness through certified courses. Georgia CR uses the University's training methodology. The trainees can build a solid foundation in the cyber-security domain through various technical or theoretical courses. The Georgia Cyber Range was added to our list, so that we can observe the big differences of the pedagogical methods the various CR use to accomplish their goals.

Table 16: Augusta University Cyber Range Mission - Capabilities – Advantages

Cyber Range	Mission	Capabilities	Advantages
Augusta University CR	Environment to support exercises and training for education and research	Certified courses with University training methodology	Complete training stack through courses

4.17 Summary of Cyber Range review

The following table demonstrates the summary of the CR review focusing on the CR goals and mission, their capabilities and advantages.

Table 17: Cyber Range Mission - Capabilities – Advantages

Platforms	Mission	Capabilities	Advantages
KYPO CR	Realistic environment for cyber-training and support for cyber-testing, research, and training for students and researchers.	Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks can be replicate for multiple and simultaneous usage	Complete training stack, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification, Capture-the-flag environment
DoD Cyber Security Range	Environment to support exercises, training, testing, evaluation, and education for the military.	Traffic generator, configurable user emulation, malware, spyware, and botnets emulation	Cyber-security and computer network defence
US Nat'l CR	Realistic environment for cyber-training and support for cyber-testing complex governmental systems.	Secure facility, role-based access, focus in cyber-security and computer network defence	Malware analysis, forensic analysis, architecture analysis, training events, research, Capture-the-flag environment, testing and product evaluation
Virginia CR	Provide an environment to increase the number, and the preparedness, of students entering the cybersecurity	Hosted in the cloud, web access, role-based access, User-specific content, dynamically creation and destruction of the virtual environments, large target networks can be replicate for multiple and simultaneous usage	Cyber-security and computer network defence, training exercises for SCADA and ICS, cyber-law and policy topics, CTF competitions

	workforce in operations		
Cyberbit CR	To provide hyper-realistic simulated training environments to enterprises, governments, academic institutions and MSSPs.	Virtual Network Replica, Attack Generator, local and remote seats for trainees, Pre-Build Networks, User Generated Networks, Pre-Build Scenarios, User generated Scenarios, inject real-life attack scenarios to the network, Realistic Traffic Generator, Knowledge base, real time monitoring, score and evaluation, Virtual and physical SCADA training, cross-functional executive training and new attack scenarios such as ransomware variants	Complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing and IR, certification courses, Capture-the-flag environment.
Raytheon CR	To provide an environment to support training and education for companies.	Network environment emulation for air traffic control, power grids, water supplies, SOCS capabilities, scalable and agile architecture, automation, interconnection with external hardware.	Reverse engineering, firmware code analysis, Radio frequency and wireless vulnerability and radiated emissions testing, cyber professional training, penetration testing, Mitigation planning and consulting, Capture-the-flag environment.
Cisco CR	To provide an environment to support training and education for the participants of an organization to combat modern cyber-threats.	Implemented with variety of application which provide visibility, intelligence, threat detection, firewalling and thread detection e.g. Cisco Stealthwatch, Cisco Splunk, Control. Includes traffic generator, configurable user emulation, malware, spyware, and botnets emulation, individual and team training, end-to-end real-time solution for machine data delivery.	Focus in cyber-security and computer network defense, threat detection, identification of various application, network traffic pattern, secure network and applications, Cisco

			Stealthwatch, Cisco Splunk, Cisco TrustSec.
ESA CR	To provide a training and simulation platform facility to provide training and testing and develop knowledge in awareness, detection, investigation, response and forensics to counter cyber-attacks specific to the space sector	Provide specialized space cyber-emulation environment to securing space assets	Instantiation of a full mission environment, mission control systems, Pre-Launch, Launch, LEOP, IOT, ground and satellite simulators, space segment, data segments, operations and development networks
CybExer CR	Environment to support training and education for companies and military.	Exercise management, red teaming capability, exercise Management Toolkit, automation, customized scenarios, GAMENET, Cyber Hygiene, Integrated Scoring and Awareness	Complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification, Capture-the-flag environment
IBM CR	Provide an environment to offer an experience in a cyber-incident	Exercise rapid-response thinking in a pressured environment, understand how security solutions work together, experience how your teams work together.	Discover gaps in enterprise's response plan, technical cyber response and leadership best practices, attacking tools, cybercrime topics, risk analysis
Palo Alto CR	To train the participants of an	Provides an isolated and realistic environment with network traffic-generator	Identify advanced attacks, mitigate

	organization to combat modern cyber-threats and enhance their prevention, detection and response skills through hyper-realistic network simulation exercises	capabilities, application traffic-generator, multiple courses.	advanced attacks, collaboration between teams, Industrial Control Systems attack scenarios, various training scenarios, Capture-the-flag environment
Silensec CR	To provide a training environment for individuals and enterprises to practice cyber-security skills in a fun and challenging way through advanced gamification modules.	Advanced monitoring, SIEM, cloud based, available as a service, support interconnection with IoT and ICS environments, competence-based scoring and assessment, virtualization automation.	Protection, detection, reaction, certifications, various training scenarios, indent response and investigations, Capture-the-flag environment and cyber-security competitions.
AIT CR	An environment for sharing the knowledge in cybersecurity domain for critical infrastructure providers, industry, research and public sector.	Advanced training exercises and competition on different levels, visualization, industrial control systems, digital networks and critical infrastructures, focus in cyber-security research and development.	Various training scenarios, offers risk assessment and evaluation modules, certifications, testing of contingency plans, incident response processes.
IXIA CR	Provide an environment to train the participants of an organization to combat modern cyber-threats using a variety of IXIA's products	Offered as a service, flexible, scalable, application and threat intelligence, visualizations modules, SIEM, traffic generator	Complete training stack, trainer console, training scenarios, advanced customization tools, various training scenarios, Capture-the-flag environment and cyber-security competitions.
NEC CR	To provide an environment to	Self-paced security challenges in various topic areas, classroom-based training for	Complete training stack through

	customers a virtualized framework for cyber-security training, modelling and simulation	different levels of expertise, team-based exercises, interconnects with physical systems.	classroom module, training scenarios, network security, penetration testing, certification, Capture-the-flag environment.
Augusta University CR	Environment to support exercises and training for education and research	Certified courses with University training methodology	Complete training stack through courses

5. STATE-OF-THE-ART CYBER RANGE

In this section, the high-level design of a state-of-the art Cyber Range will be described. Furthermore, its module will be analysed and compared with the reviewed Cyber Range of section one. A state-of-the-art Cyber Range should be a federated solution, in order to enhance all the appropriate skills of cyber-security specialists. The trainees must develop analytical skills in various domains at all levels (from junior to senior), such as:

- Prevention for identification and mitigation of the vulnerabilities and threats.
- Detection for simulating and analysing attack patterns.
- Reaction for rapid response and robust recovery.

The training must be realistic and the simulated platform should combine a holistic approach of cyber-security domains in various critical infrastructures. A hybrid model of cyber-security defence and response is emerging; for that reason, the training scenarios should consist of more than one critical infrastructure from power grid and IoT to naval and aviation. To accomplish the above, a state-of-the-art Cyber Range should be able to interconnect with other Cyber Range infrastructure, in order to be able to create realistic and dynamic scenarios based on identified and forecasted cyber-attacks and vulnerabilities. Cyber-threat intelligence that is gathered from various sources and evaluated and analysed must be implemented for the creation of new training scenarios, so that the cyber-security specialists can follow the scourges and evolution of the threats. Furthermore, it must provide threat and risk analysis models, which aim at identifying the valuable assets, threats, variability, and at estimating the probability of threat appearance, identifying the potential impacts and measuring the consequences of a cyber-attack. With the above requirements, the platform should aim at a holistic approach to cyber-threat management, focus on research of the current cyber-threats and prepare the trainees for the upcoming.

5.1 Modules of the Cyber Range

New technologies require innovative ways to implement security measures. The cyber-security professionals must develop skills that will allow them to identify threats and take proper mitigation actions. The need to estimate and forecast the impacts of a cyber-attack in an organization is now mandatory. The cyber-security experts must adapt to a constantly evolving landscape where cyber-attacks are increasing in sophistication and scale, while they should be able to face the quick rate of cyber-threat evolution. As a result, various tools, techniques and modules must be implemented. From the European Commission research and innovation call SU-DS01-2018: Cyber-security preparedness - cyber range, simulation and economics [36] the following modules can be extracted:

- Cyber-threat intelligence gathering, sharing, discovery zero-day vulnerability module.
- Threat forecasting module.
- Cyber-security visualization module.

- Gamification module.
    - Dynamic and automated scenario, topologies, exercise generation.
    - Complex training scenario creation in multiple domains.
- Risk analysis and assessment module.
- Forensic evidence collection module.
- Interconnection with external platforms.

Cyber-threat intelligence focuses on the collection and analysis of information about current and forthcoming attacks. Cloud Computing, critical infrastructures, social media, smartphones and IoT are examples of emerging technologies where sophisticated attacks have occurred. The new-generation threats are multi-vector, as they can use multiple means of propagation and multistage, because they utilize multiple phases for infiltrating the networks, spreading, and exploiting the valuable data [37]. A cyber-threat intelligence module should be able to gather and share the latest zero-day vulnerabilities and social engineering techniques to give an in-depth understanding of those threats and even be able to discover them. Analysing current cyber-threats is an important method for understanding the evolution of the cyber-incidents [38]. Modelling simulation and analysis of the current cyber-threats allow forecasting of the cascading effects that would result from successful cyber-attacks. A threat forecasting module can provide knowledge from understanding the system security baseline to identifying and prioritizing remediation actions [39]. To enhance the situational awareness of cyber-security analysts, visual analytics platforms will provide effective ways for presenting alert zones, events, attack evolution and malware propagation paths. The visual analytics platform joins and links multiple information visualization views and a multi-display system [40]. According to National Institute of Standards and Technology (NIST), risk assessments are used to identify, estimate and prioritize risk to organizational operations [41]. A risk analysis and assessment module can enhance the trainee's ability to identify the key assets of a critical infrastructure and, with the cooperation of the other modules, it gives them the ability to implement security policies and measures that will protect from forthcoming threats.

Since the last decade, gamification has been applied in security education and training. Capture-the-flag events that use gamification and game-based learning for teaching computer security topics are becoming more and more popular, e.g. in DEF CON qualifiers, more than five hundred teams competed [42]. Emerging technologies have changed digital forensic spectrum from cloud computing to IoT-based ecosystems. Nowadays, it is essential for trainees to understand the fundamental areas in digital forensics and deepen their knowledge in more complicated subjects, such cloud computing and infrastructure as a service (IasS), platform as a service (PaaS) and software as a service (Saas) [43]. Data integrity and encryption deletion in a visualized environment create various challenges that the trainees must overcome. The interconnection module will provide the platform with high availability, load balancing and scalability, supporting multi-domain cyber-security training exercises of any scale.

5.2 Cyber-threat Intelligence gathering, sharing, discovery zero-day vulnerability module

Sharing security knowledge between experts across organizations is essential. Cyber-threat intelligence refers to the evidence-based knowledge about existing or forthcoming threats, gathered from a range of open-source intelligence, dark web or other intelligence gathering structures, which aims to identify, characterise and prove ongoing or forthcoming threats. Many organizations implement CTI gathering as a prevention mechanism against emerging attacks. Computer Emergency Response Teams gather and share information about new threats or warnings. Computer Security Incident Response Team is responsible for receiving, responding and validating cyber-incidents and activities. Law enforcement Teams (LEAs) are even more connected with cyber-incidences and have great responsibility to protect their countries against cyber-threats. The Forum of Incident Response and Security Teams (FIRST) joins a variety of computer security incident response teams from government, commercial and educational organizations. As a result, a cyber-threat intelligence module is essential for a state-of-the-art Cyber Range platform, which must be connected to all the above organizations and institutes for sharing, gathering or even discovering zero-day vulnerabilities. That module can depend on open-source platforms [44], such as:

(i) The Malware Information Sharing Platform (MISP) [45], which is a threat intelligence platform for gathering, sharing, storing and correlating indicators of compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information,.

(ii) The Collaborative Research into Threats (CRITs) [47], which is an open-source malware and threat repository.

(iii) The Financial Services Information Sharing and Analysis Center (FS-ISAC) [47], which is a forum for collaboration on critical security threats faced by the global financial services sector.

(iv) (iv) the Collective Intelligence Framework (CIF) [48], which combines known malicious threat information from many sources.

(v) The GOSINT [49] framework, which is a project used for collecting, processing, and exporting high quality indicators of compromise,.

(vi) The MineMeld [50], which is a community-supported tool to handle a list of indicators and transform/aggregate them for consumption by third-party enforcement infrastructures.

The need for a threat intelligence module to automatically collect intelligence from custom or public sources and automatically update and further enhance the collected intelligence is considered vital. The collected information will also feed the other modules of the platform for the creation of cyber-security exercises. (For further needs, STIX, TAXXI, CybOX may be used.) The proposed architecture for the cyber-threat intelligence module also includes a module (*Ambassador*) which is responsible for the interconnection with CERTs CSIRTs LEAs.

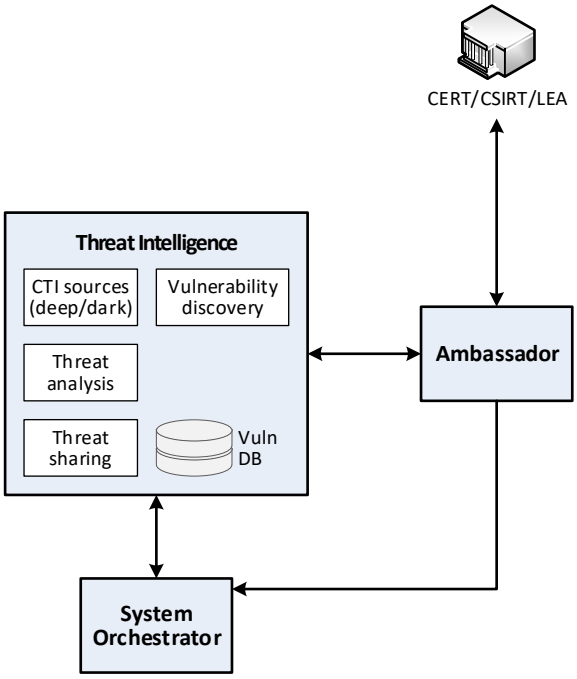

Figure 1: Cyber-threat Intelligence gathering, sharing, discovery zero-day vulnerability module

5.2.1 Comparing the reviewed Cyber Ranges as to the inclusion of threat intelligence functionality

For a Cyber Range to be qualified for the inclusion of Threat Intelligence capabilities, the platform should be able to store and *share* cyber-security intelligence and incident reports, to *gather* and *analyse* information both from internal and external sources, or even to be able to *discover* zero-day vulnerabilities.

Table 18: Threat intelligence functionalities

Platform	Gathering	Sharing	Analysis	Discovery
KYPO CR	N	N	N	N
DoD CR	Y	Y	Y	Y
US Nat'l CR	N	N	N	N
Virginia CR	N	N	N	N
Cyberbit CR	N	Y	Y	N
Raytheon CR	N	N	N	N
Cisco CR	Y	Y	Y	Y

ESA CR	N	N	N	N
CybExer CR	N	N	N	N
IBM CR	N	N	N	N
Palo Alto CR	Y	Y	Y	N
Silensec CR	Y	Y	Y	N
AIT CR	N	N	N	N
IXIA CR	Y	Y	Y	N
NEC CR	N	N	N	N
Augusta U. CR	N	N	N	N

*Note: **Y**es; **N**o*

The following graph demonstrates the number of Cyber Ranges that include cyber-threat intelligence gathering, sharing, analysis and discovery functionalities. Six of the reviewed Cyber Ranges include some of the required features, but only two include threat discovery.

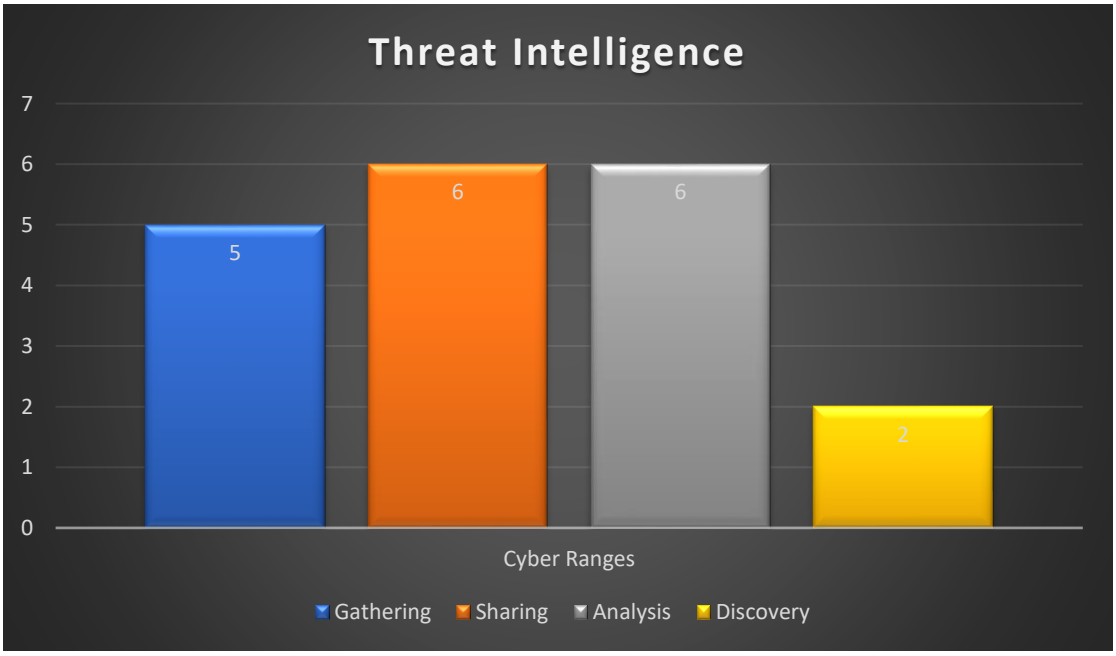

Figure 2: Threat Intelligence representation per Cyber Range

5.3 Threat forecasting module

In a state-of-the-art Cyber Range, a threat forecasting module is considered vital. The collected intelligence from the CTI module and the collected net-flow samples from various attacks will feed the threat data visualization tools, threat simulation tools and threat forecasting tools. Cyber-security data also coming from other sources, such as incident reports, research, statistics, statistical modelling and expert knowledge, will be used and analysed. Big Data and machine learning can enhance this process by learning how to automatically detect unusual patterns in web traffic. The huge raise of encrypted traffic during last year [51] makes machine learning really valuable because of its capability of monitoring previously unseen encrypted network traffic. A threat Forecasting module can help to improve the security posture prior to an attack. The holistic view with the gathered intelligence accompanied with the data analysis of the pattern and trends of the attacks, and the network flow analysis of machine learning will improve the cyber-security awareness of trainees and they will be able to build a threat modelling for their needs off proactive data driven by big-data analysis.

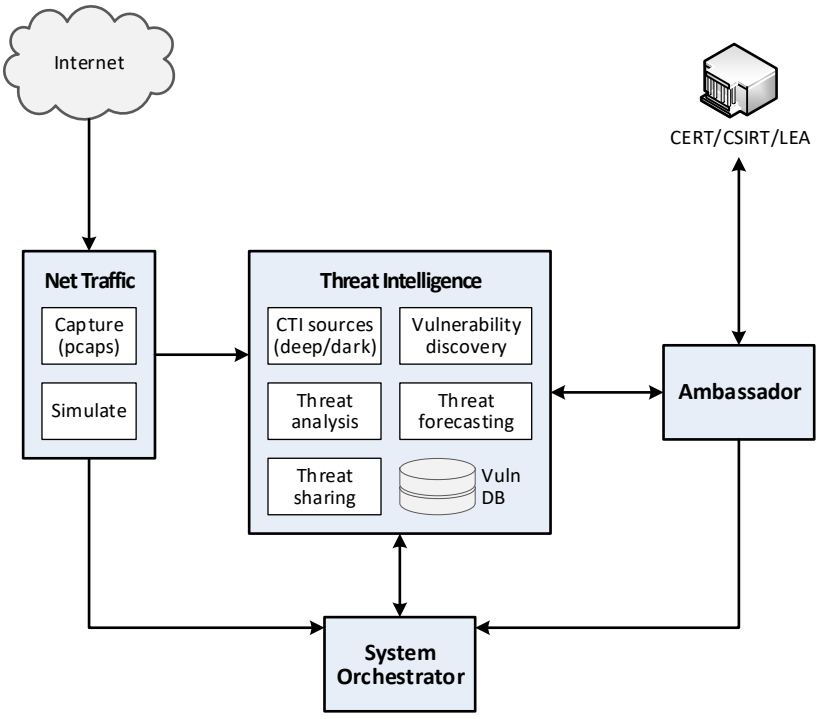

Figure 3: Adding Threat forecasting module

5.3.1 Comparing the reviewed Cyber Ranges as to the inclusion of threat forecasting

As mentioned in threat forecasting, it is vital to *gather, analyze* data flows from internal and external sources and be able to *detect* unusual network traffic patterns. A state-of-the-art Cyber Range should extend the capabilities of existing cyber ranges and allow the

creation of complex cross-domain scenarios that are based on identified and forecasted trends and needs.

Table 19: Threat forecasting functionalities

Platform	Traffic gathering	Net flow Analysis	Detection
KYPO CR	N	N	N
DoD CR	Y	Y	Y
US Nat'l CR	N	N	N
Virginia CR	N	N	N
Cyberbit CR	N	N	N
Raytheon CR	N	N	N
Cisco CR	Y	Y	Y
ESA CR	N	N	N
CybExer CR	N	N	N
IBM CR	N	N	N
Palo Alto CR	Y	Y	Y
Silensec CR	N	N	N
AIT CR	N	N	N
IXIA CR	Y	Y	Y
NEC CR	N	N	N
Augusta U. CR	N	N	N

*Note: **Y**es; **N**o*

The following graph demonstrates the number of Cyber Ranges that include cyber-threat forecasting functionalities. Only four of the reviewed Cyber Ranges include threat forecasting functionalities in their infrastructure, but all of them include traffic gathering, net flow analysis and detection.

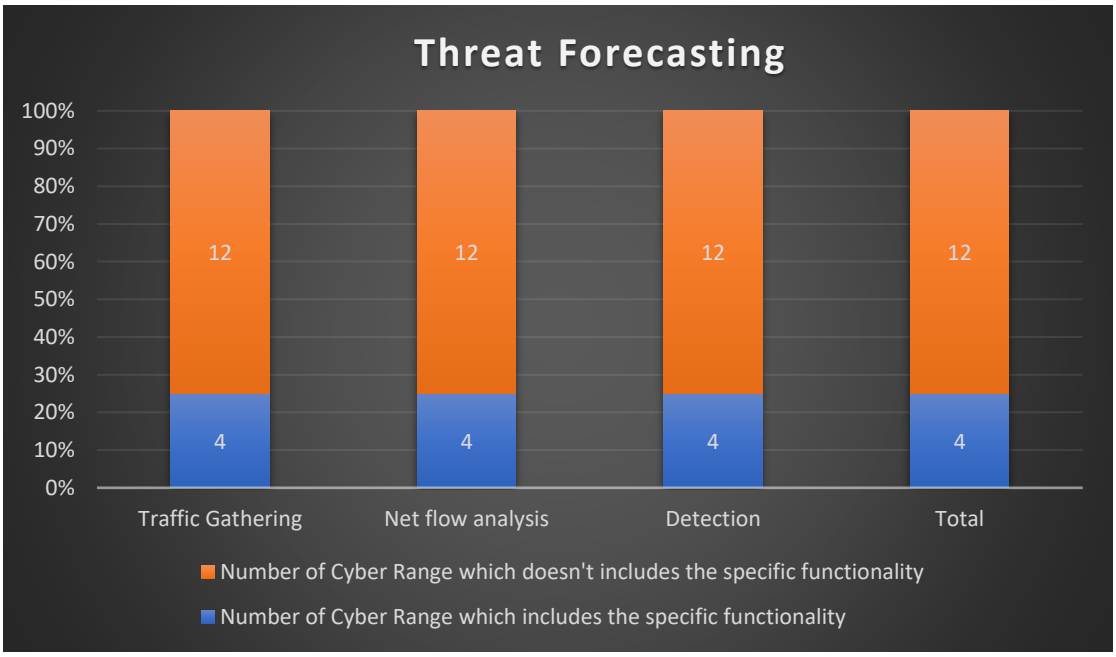

Figure 4: Threat Forecasting representation per Cyber Range

5.4 Visualization module

The visualization features of a Cyber Range offer effective ways for presenting alert zones, events, attack evolution, malware propagation paths and correlations with CTI. This module interworks with threat forecasting and threat intelligent modules and aims at assisting trainees in understanding attack origins and patterns, and in increasing their capabilities to predict attack patterns and their further development. Visualization features are particularly important considering the high volume of data that security experts need to review and evaluate during a cyber-attack. Furthermore, data visualization can help security specialists understand an attack and prevent its reoccurrence. Complex malware data can be visualized as a graph and, with additional software features, it is possible to reveal network structures that can pinpoint trends and entry points in a network [52]. Security Information and Event Management (SIEM) tools can be used for the data visualization module. Visualization in cyber-security is not only required for alerting and visualizing network traffic and malware propagation. SIEM combines security tools under one framework, such as: (i) Security Information Management (SIM), (ii) Security Event Management (SEM), (iii) Log management (LMS). The correlation of events from the different data sources like CTI and historical data is mandatory for the creation of this module. AlienVault OSSIM [53] is an open SIEM that provides event collection, normalization and correlation. The Elastic Stack [54] (ELK stack) is defined by three open-source projects: Elasticsearch, Logstash and Kibana. Elasticsearch is a search and analytics engine that can be fed with data from Logstash, which ingests data from multiple sources and visualizes the results with Kibana. The SiLK is a collection of open-source traffic collection, processing, storage and analysis tools that can combine with various research projects, such as VIAssist [40], for the creation of a visual analytics platform.

The visualization module that will be selected or implemented must scale to large data sources and be easily understandable by trainees [55]. (For further needs, OSSEC, Apache Metron, Prelude can be used.)

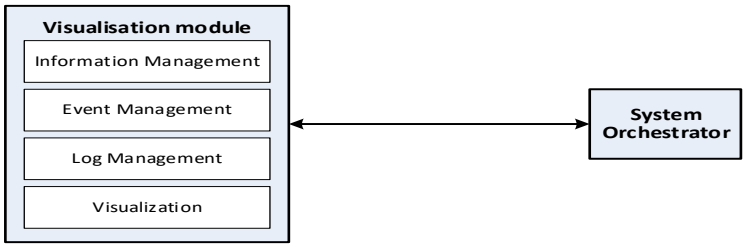

Figure 5: Visualization module

5.4.1 Comparing the reviewed Cyber Ranges as to the inclusion of visualization module

Cyber ranges deal with time-evolving data, often of very large amounts of *information*, *events* and *loggings*. Making any sense of these data in raw, textual format is almost impossible. *Visualisations* can present such data in easily comprehensible graphical representations and are therefore very effective tools for understanding the data. Interactive visualisations are even more useful.

Table 20: Visualization functionalities

Platform	Information Management	Event Management	Log Management	Visualization
KYPO CR	N	N	N	N
DoD CR	Y	Y	Y	N
US Nat'l CR	N	N	N	N
Virginia CR	N	N	N	N

Cyberbit CR	N	N	N	Y
Raytheon CR	N	N	N	N
Cisco CR	Y	Y	Y	Y
ESA CR	N	N	N	N
CybExer CR	N	N	N	N
IBM CR	N	N	N	N
Palo Alto CR	Y	Y	Y	Y
Silensec CR	Y	Y	Y	Y
AIT CR	Y	Y	Y	Y
IXIA CR	Y	Y	Y	Y
NEC CR	N	N	N	N
Augusta U. CR	N	N	N	N

*Note: **Y**es; **N**o*

The graph below demonstrates the number of Cyber Ranges that include visualization functionalities. Only four of the reviewed Cyber Ranges include a complete visualization module and six of them include some of the required features.

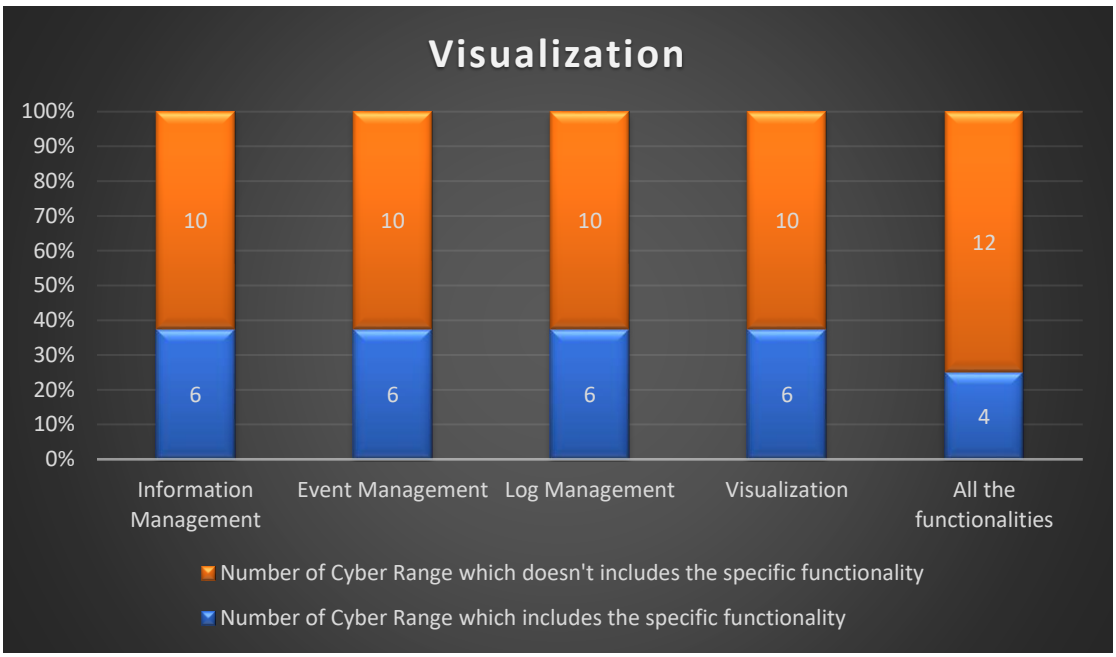

Figure 6: Visualization representation per Cyber Range

5.5 Gamification module

Gamification has been defined as " the use of game design elements in non-game contexts" [56]. Various methodologies have endeavoured to introduce gaming components in cyber-security education. These methodologies vary from using simple games for beginners and non-experts to cyber-security training ecosystems for cyber-security professionals. Through gamification, trainees can obtain the appropriate practical skills as well as the corresponding theoretical knowledge. A problem-solving mechanism through lab-environments enables the participants to be a part of the problem – solution in a cyber-security incident, which increases cyber-resilience and their creative-thinking methods. Most of the game genres can be applicable to cyber-security training. Casual games that tend to be easy to learn and not difficult to master can improve cyber-security awareness, e.g. GAP [57], which is a web-based game for improving awareness of passwords and aims at making players aware of bad password decisions. Action games, whose main mechanics involve movement, accuracy, decision and reaction time, can improve trainees' attack capabilities with a time limit, e.g. gaining access to an infrastructure before the time ends (certification preparation like OSCP). Role Playing Games (RPGs), where the trainee controls a fictional character that undertakes a quest in an imaginary world, can provide a complete cyber-security training stack, e.g. The Necromancer [58], which involves from port-scanning to web penetration testing. Strategy games, whose main aspect is to balance in a specific territory with the goal of obtaining it, can improve decision-making and cyber-defence training. Fighting games are applicable in Red vs Blue team scenarios or Capture-the-Flag scenarios. Open-world games, whose main characteristic is the player's freedom of movement, action and decision against the environment, can provide a complete training stack and certification preparation for individuals and teams, and they are also applicable in Red vs Blue team scenarios or Capture–the-Flag scenarios. As a result, security awareness can be

obtained from simple board games e.g. Cryptomancer RPG [59], which covers topics such as symmetric and asymmetric encryption or Control-Alt-Hack[60], or more cutting-edge-technology games, such the proposal of Salazar [61], which is an augmented reality-based game.

One of the most difficult problems is the creation of exercises with high-quality pedagogical, educational training process in the Cyber Range environments, as the simulated systems are closed and isolated from the internet [62]. The training exercises must be real-life scenarios applicable to real critical infrastructures.

For the configuration of the training environment, the following should be taken into consideration:

- The training exercises should be automatically deployed and the underlayer environment should automatically be created, while training exercises should be injected to the automatically created virtualized environment.
- The challenges should be able to be reused. Restarting mechanisms should apply without the creation of a new environment.
- The platform should maintain a low cost of power, processing power, memory and storage. Deallocation mechanisms of inactive sandboxes should be used.
- The platform should have high-availability redundancy mechanisms. Cloning challenges and progress should be considered.

As far as the training exercises are concerned, the following should be taken into consideration:

- The environment should support a variety of challenges, such us Web Applications, Forensics, Cryptography, Steganography, Exploitation etc. (see *ANNEX 1*).
- The training must be linked to professional certification programs.
- The challenges must have levels of difficulty, so that the trainee can train in the same exercise, in the same domain, in a range of levels of difficulty.
- The challenges must support modes such as training with instructor, instructorless, self-passed, single-person challenges, team challenges, player vs player challenges, team vs team challenges, player vs infrastructure challenges etc. The three main pillars are: i) Individual Skills for standalone cyber-security techniques, ii) Team Skills for cooperation and communication, iii) Computer Security Incident Response Team: advanced team skills.
- The challenges must support hands-on practice with the appropriate theoretical domain.
- The challenges must be relevant to the critical infrastructure that is deployed.

For the training exercises content, the following should be taken into consideration.

- *Attack-oriented training,* which provides the experience of recreating vulnerability exploitation techniques and includes activities such as penetration testing, which make use of the same tools and methodologies that attackers deploy.
- *Defense-oriented training,* which focuses on the design and implementation of vulnerability protection mechanisms, so as to prevent similar future attacks.

- *Analysis/forensics-oriented training,* which aims at cultivating a deeper understanding of the phenomena related to vulnerability exploitation and patching, including the identification of targeted attack campaigns [63].

The main goals of the gamification module follow the principles below and, to accomplish them, various sub-module or APIs are interconnected. A state-of-the-art CR and its components must achieve:

- *Flexibility*: The number of network topologies and the network elements that are supported as well as the supported operating systems. The ability of creation of dynamic network topologies as well as replicas of existing networks.
- *Scalability*: The platform should scale well in terms of: number of topology nodes, processing power, network size and number of simultaneous users.
- *Automation*: The allocation - deallocation of the resources as well as the created scenarios and exercises must be created in an automated way.
- *Isolation*: The core components of the platform and especially the created lab environments as well as the generated toolkits should be isolated from the real world.
- *Interoperability*: Integration with external systems should be able to be achieved (Interconnection with external Cyber Range module).
- *Effectiveness*: The platform should cover plenty theoretical and practical Training Domains and, if possible, cover several critical infrastructures.
- *Realism*: The created scenarios and exercises must be able to simulate – emulate a real infrastructure.
- *Monitoring*: Real-time and historical data for the platform’s infrastructure, training process, user’s behavior etc.
- *Access*: Users should access the platform in various ways, e.g. VPN, webpage.
- *Service-based Access*: Depending on the roles of a user, different privileges must be given in service access.
- *Scoring and Evaluation*: Users’ scoring and evaluation results depending on their decisions.
- *Risk Evaluation*: The platform should be able to identify, analyse and evaluate the risk of a cyber-threat [64][65] (Risk analysis and assessment module).

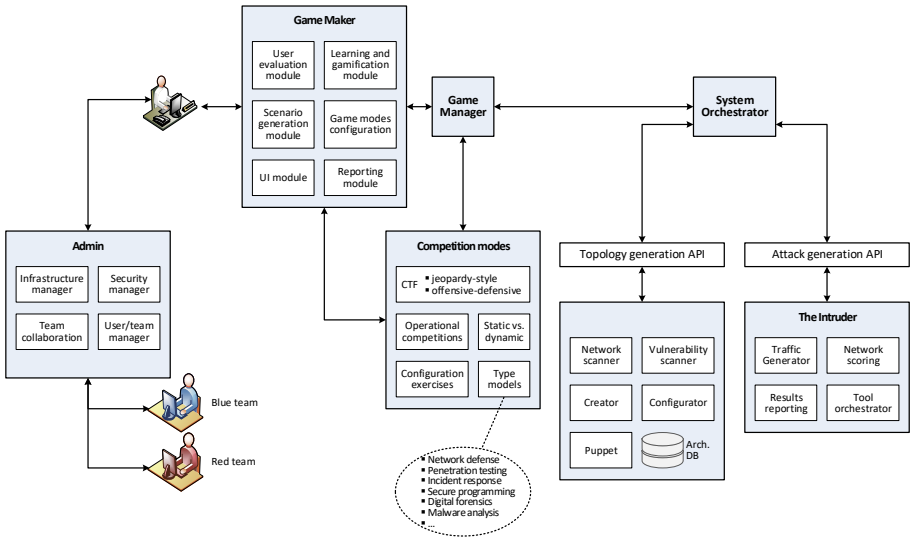

Figure 7: Gamification module

5.5.1 Comparing the reviewed Cyber Ranges as to the inclusion of gamification characteristics

It is essential for a CR platform to include the major characteristics that have been described in the gamification module. Gamification will leverage the interactivity of the training process, enhance the trainees' overall learning experience and promote trainee engagement. As a result, the training outcomes will be maximized. A flexible and scalable isolated virtual training environment is needed for the creation of hyper-realistic training exercises in an automated way.

Table 21: Gamification characteristics

Platform	Flexibility	Scalability	Automation	Isolation	Effectiveness	Realism	Monitoring	Visualization	Access	Serviced based access	Scoring and evaluation
KYPO CR	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
DoD CR	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y
US Nat'l CR	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
Virginia CR	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y
Cyberbit CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Raytheon CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cisco CR	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y
ESA CR	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
CybExer CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IBM CR	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y
Palo Alto CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Silensec CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
AIT CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IXIA CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NEC CR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Augusta U. CR	N	N	Y	Y	N	N	Y	Y	Y	Y	Y

*Note: **Y**es; **N**o*

The following graph demonstrates the number of Cyber Ranges that include the described gamification characteristics. The lack of cross-domain exercises as well as the lack of real network traffic generator in the created scenarios affect the effectiveness and realism of the created training exercises.

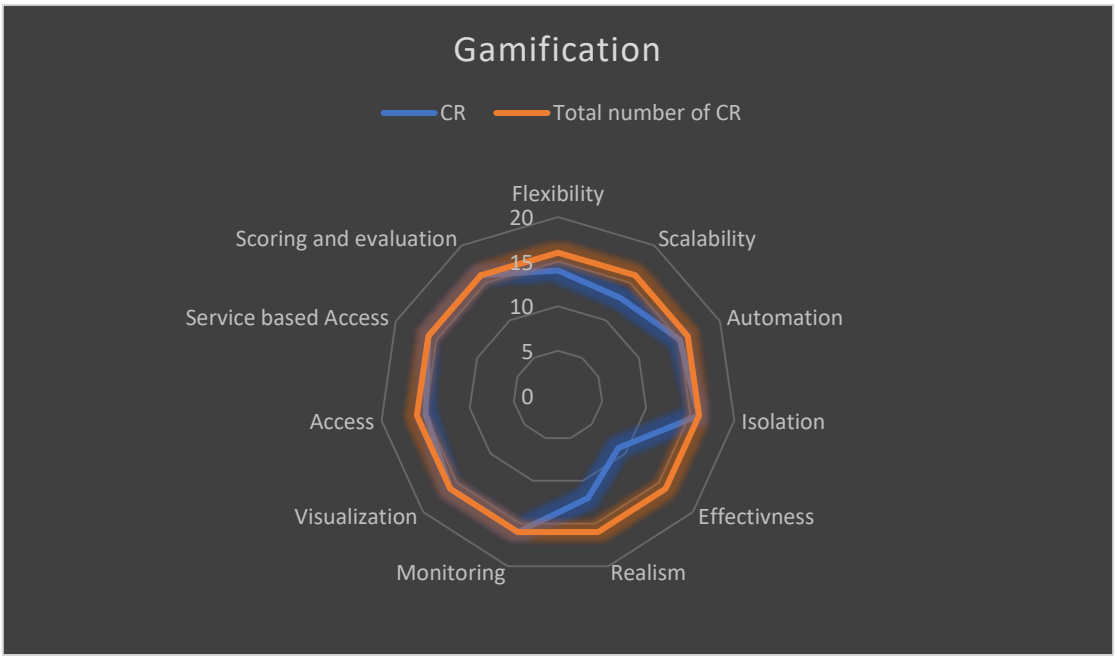

Figure 8: Gamificationn representation per Cyber Range

5.6 Risk analysis and assessment module

A cyber-security risk assessment identifies the assets in an organization's critical infrastructure that could be affected by an attack and then identifies the risks that could affect those assets. According to NIST, risk assessments are used to identify, estimate and prioritize risks to organizational operations (i.e. mission, functions, image and reputation), organizational assets, individuals, other organizations and the Nation, resulting from the operation and use of information systems [66]. The effectiveness of mitigation methods can be enhanced by identifying, analysing and understanding not only the threats, but also the associated risk. Risk assessment methods are in general classified into qualitative [67] and quantitative [68]. While qualitative methods use a subjective risk classification (e.g. low–medium–high), quantitative methods aim at calculating the risk numerically [69]. The risk models of a state-of-the-art Cyber Range must be quantitative and take in consideration the impact of cyber-incidents and associate it with threats and vulnerabilities. Model-based method risk analysis is based on graphs and supports mathematical models, and an attack tree provides the view of the events leading to an attack [70]. A risk assessment method based on an Attack Countermeasure Tree (ACT) is a combination of attack, detection and mitigation events [71]. Using a quantitative risk analysis method, the module will be more pedagogical, demonstrating how the changes in the simulation scenario can affect the overall risk. In the automatically generated simulated scenarios or in the network replicas of real organizations' networks, the valuable assets, the possible threats, the vulnerabilities and possible intrusion points can be defined and analysed as to the risk of various cyber-attacks. A cyber-risk assessment model should be supported by forensics, for analysis of cyber-attacks and information sharing with the CTI [72].

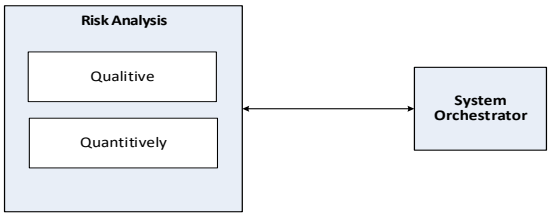

Figure 9: Risk analysis and assessment module

5.6.1 Comparing the reviewed Cyber Ranges as to the inclusion of Risk analysis and assessment module

Risk analysis and assessment aims to analyse cyber security problems including important assets, main threats and vulnerabilities in a critical infrastructure. Risk assessment is the foundation of the study for cyber security in Industrial Control System [73].

Table 22: Risk analysis and assessment characteristics

Platform	Qualitive	Quantitively
KYPO CR	N	N
DoD CR	N	N
US Nat'l CR	N	N
Virginia CR	Y	N
Cyberbit CR	Y	N
Raytheon CR	Y	N
Cisco CR	N	N
ESA CR	N	N
CybExer CR	Y	Y
IBM CR	N	N
Palo Alto CR	N	N
Silensec CR	Y	N
AIT CR	Y	N
IXIA CR	N	N
NEC CR	N	N
Augusta U. CR	N	N

*Note: **Y**es; **N**o*

The following graph demonstrates the number of Cyber Ranges that include risk a analysis module, quantitative or qualitative.

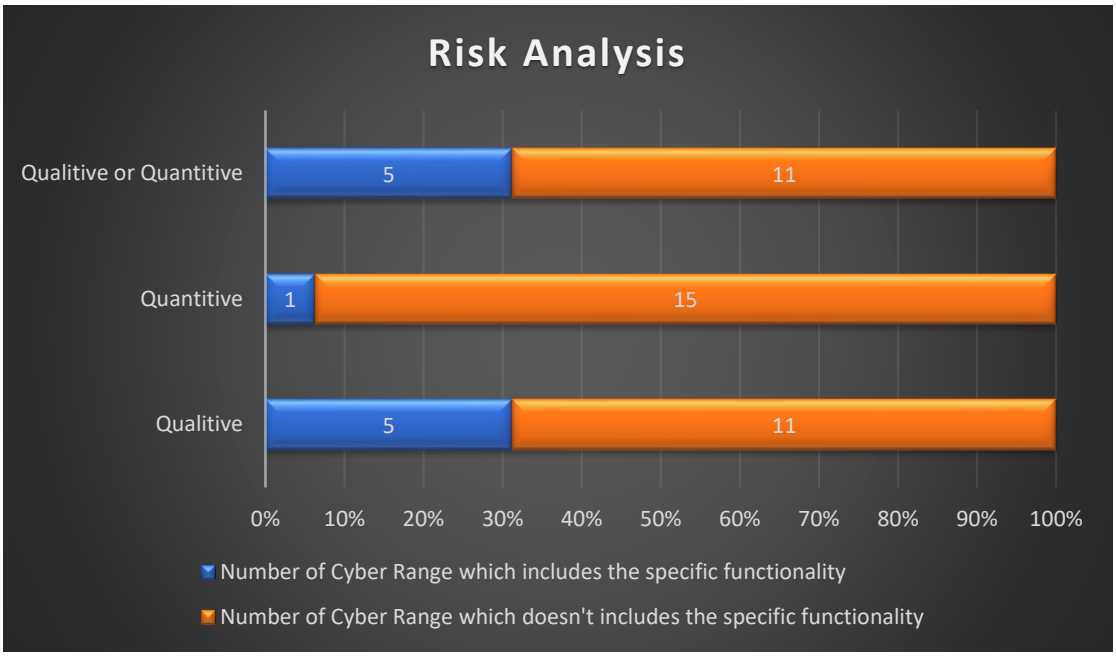

Figure 10: Risk analysis and assessment representation per Cyber Range

5.7 Forensic evidence collection module

Digital Forensics can be defined as the process of identification, collection, examination and analysis of data by preserving the data integrity and maintaining security [74]. With the advent of modern computing, a new landscape of cyber-threats has created the need to gather new forms of forensic evidence into a vital tool. To support this new discipline, specialized tools have also emerged to assist investigators in capturing, analysing and preserving the evidence that might arise during the course of investigating the cyber-incidence that has occurred. Any part of an enterprise system can be vulnerable to a cyber-threat, data theft or unauthorized penetration. A forensic analyst must make sure to analyse storage media hardware and operating systems, networks and applications, in order to locate the point of compromise. The digital forensic process, which covers the entire evidence gathering procedure, can be divided into parts, from data collection to examination and analysis, and reporting. Computer systems, networks and mobile devices can all be utilized in or fall victim to a cyber-attack. Each device type has different intrusion methods, and the requirements for evident handling this have led to the development of three distinct branches of digital forensics. Computer forensics may rely on the need to create a disk image, in order to preserve evidence, or virtual drives may be used to emulate an entire machine. Network forensics focuses on the monitoring and analysing of computer network traffic. Mobile devices present their own unique challenges due to memory volatility. In an increasingly complex and fast-moving technological landscape, cyber-threats are becoming more sophisticated and data breaches are becoming more damaging to enterprises. Therefore, it is essential that

digital forensics training process is evolved too, so that the cyber-security professionals can face the upcoming incidents. This necessary evolution in the digital forensics process is described for various new infrastructures, such as a smart-home environment [75], where a new methodology approach has been proposed. An overview of proactive forensic solutions and its applicability to 5G [76] and how important it is to prepare the 5G ecosystem for digital forensics, the correlation of the evidence in a multi-layer resource-sharing infrastructure such as cloud computing [77] are some examples of the evolution of digital forensics. Open-source solutions can be used for network traffic and indexing, such as Moloch [78]. For intrusion detection, security monitoring, and log management, Security Onion [79] can be utilized, which is a Linux distribution, or OSSEC[80], which is an IDS that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response, or other evidence collection mechanisms and tools for a semi-automated evaluation, such as a probe, a malware analysis system, a correlation engine, an incident management system or a honey pot.

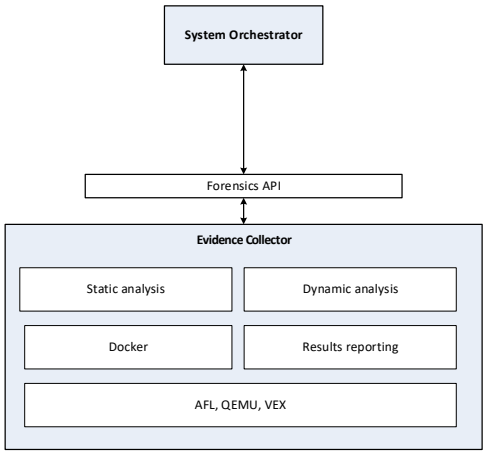

Figure 11: Forensic evidence collection module

5.7.1 Comparing the reviewed Cyber Ranges as to the inclusion of Forensic evidence collection module

As mentioned above, the digital forensic *process* that covers the entire evidence gathering procedure can be divided into parts, from data collection to examination and *analysis, reporting (real time alerting and monitoring)* and correlation.

Table 23: Forensic evidence collection characteristics

Platform	Process	Analysis	Policy	Alerting	Correlation Engine
KYPO CR	Y	Y	N	N	N
DoD CR	Y	Y	Y	Y	N
US Nat'l CR	Y	Y	N	N	N
Virginia CR	Y	Y	N	N	N
Cyberbit CR	Y	Y	Y	Y	N
Raytheon CR	N	N	N	N	N
Cisco CR	N	N	N	N	N
ESA CR	Y	Y	Y	N	N
CybExer CR	Y	Y	N	N	N
IBM CR	N	N	N	N	N
Palo Alto CR	N	N	N	N	N
Silensec CR	Y	Y	N	N	N
AIT CR	Y	Y	N	N	N
IXIA CR	Y	Y	Y	Y	Y
NEC CR	N	N	N	N	N
Augusta U. CR	N	N	N	N	N

*Note: **Y**es; **N**o*

The following graph represents the number of Cyber Ranges that include forensic evidence collection characteristics. Most of the Cyber Ranges that include a forensic evidence collection module focus on log analysis and forensic process.

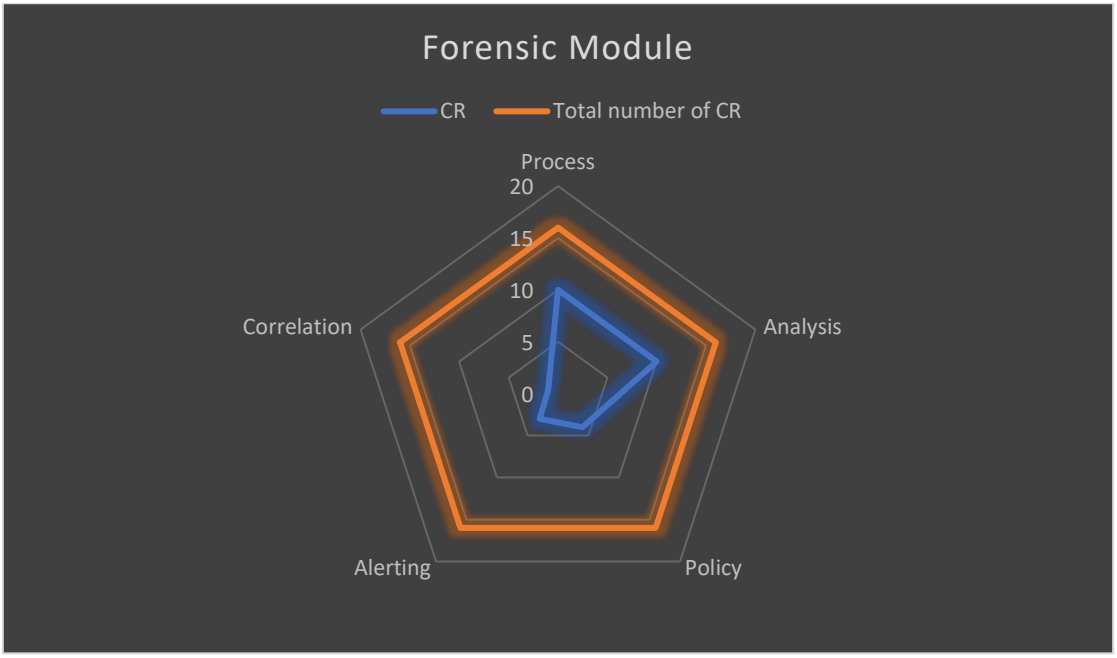

Figure 12: Forensic evidence collection representation per Cyber Range

5.8 Interconnection with external platforms

A state-of-the-art Cyber Range must function as a stand-alone range or be interconnected with other cyber-simulators or ranges. Through cyber-range interconnections, a wider range of training material will be available to trainees, allowing them to obtain cyber-security training regarding a broader spectrum of cyber-attacks. This is highly important, since contemporary systems become more complex and more interconnected. In an increasingly complex technological landscape, such interconnection with external simulators or ranges will provide high availability, load balancing and scalability, supporting multi-domain cyber-security training exercises of any scale, which will ensure that platform users will be better prepared to defend against even the most sophisticated cyber-attacks. Such interconnection should be achieved in many layers: Infrastructure layer for the allocation of the compute and storage resources of the CR, which will provide high availability, load balancing, and scalability. Physical interconnection, such as next-generation firewalls, traffic generators, network elements, IoT and ICS environments that cannot be simulated will provide multi-vendor training and hyper-realistic scenario creation. Application layer, where the CR will interconnect with the third-party applications and training contents, which will provide a more holistic approach than different training perspectives. Simulated environment interconnection, where the CRs are interconnected for the creation of hybrid scenarios and training exercises in multiple training domains.

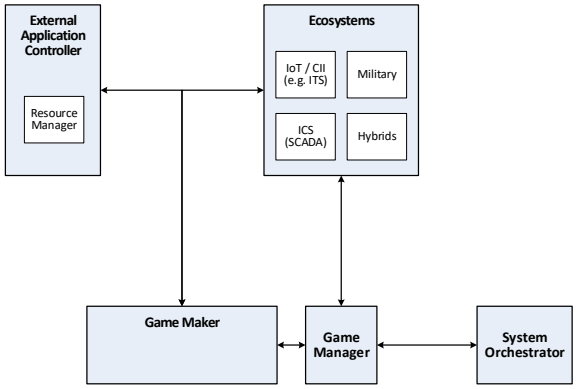

Figure 13: Interconnect module

5.8.1 Comparing the reviewed Cyber Ranges as to the inclusion of interconnection capabilities

For a CR platform to ensure its self-preservation, it should be able to interconnect with external *Infrastructure*. *Physical* interconnection with external devices will provide multi-vendor training and hyper-realistic scenario creation. *Application*s interconnection will provide various training capabilities. *External CR* interconnection will provide hybrid scenarios and training exercises in multiple training domains.

Table 24: Interconnection characteristics

Platform	Infrastructure	Physical	Application	External CR
KYPO CR	Y	N	N	N
DoD CR	Y	Y	N	N
US Nat'l CR	N	N	N	N
Virginia CR	Y	Y	Y	N
Cyberbit CR	Y	Y	Y	N
Raytheon CR	Y	Y	Y	N

Cisco CR	Y	Y	N	N
ESA CR	Y	Y	Y	N
CybExer CR	N	N	N	N
IBM CR	N	N	N	N
Palo Alto CR	Y	Y	N	N
Silensec CR	Y	Y	Y	N
AIT CR	Y	Y	N	N
IXIA CR	Y	Y	N	N
NEC CR	Y	Y	Y	N
Augusta U. CR	N	N	N	N

*Note: **Y**es; **N**o*

The graph below demonstrates the number of Cyber Ranges that include an interconnection module. Most of the reviewed Cyber Ranges focus on infrastructure and physical, and none of them have interconnection with external Cyber Range capability.

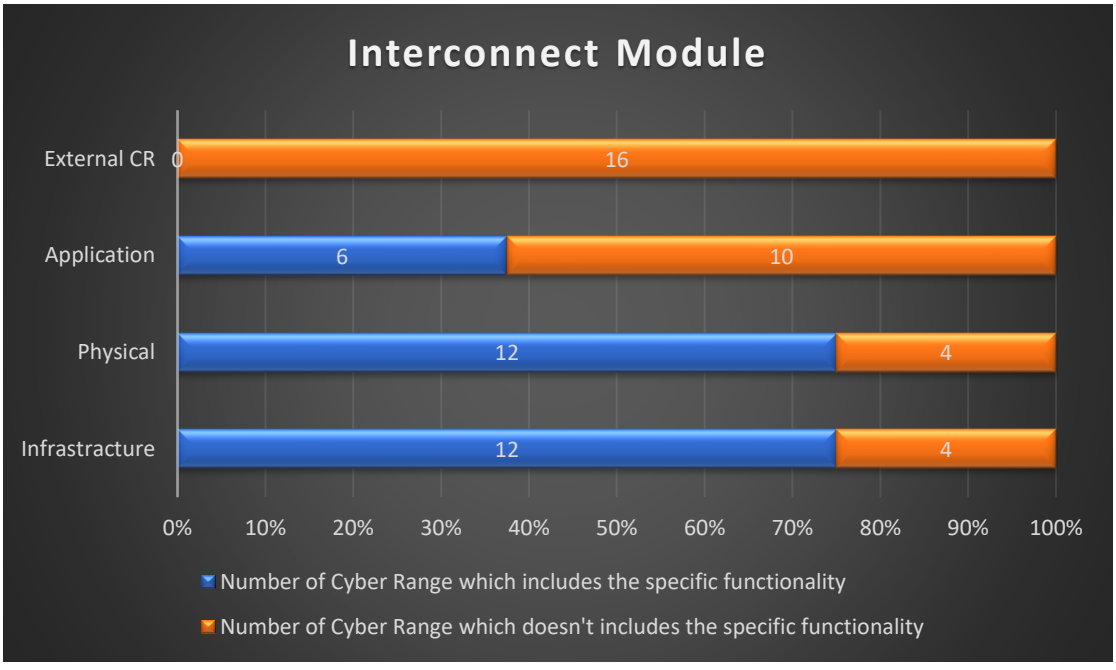

Figure 14: Interconnection representation per Cyber Range

5.9 Demonstration of the complete architecture

In figure 15 the compete architecture is demonstrated. The described modules from the previous sections are combined for the creation of the complete high-level architecture. The two major modules which are responsible for the interconnection with the rest modules are the system orchestrator and the game manager. Ambassador is responsible for the external interconnections such as LEAs/CERT/CSIRT.

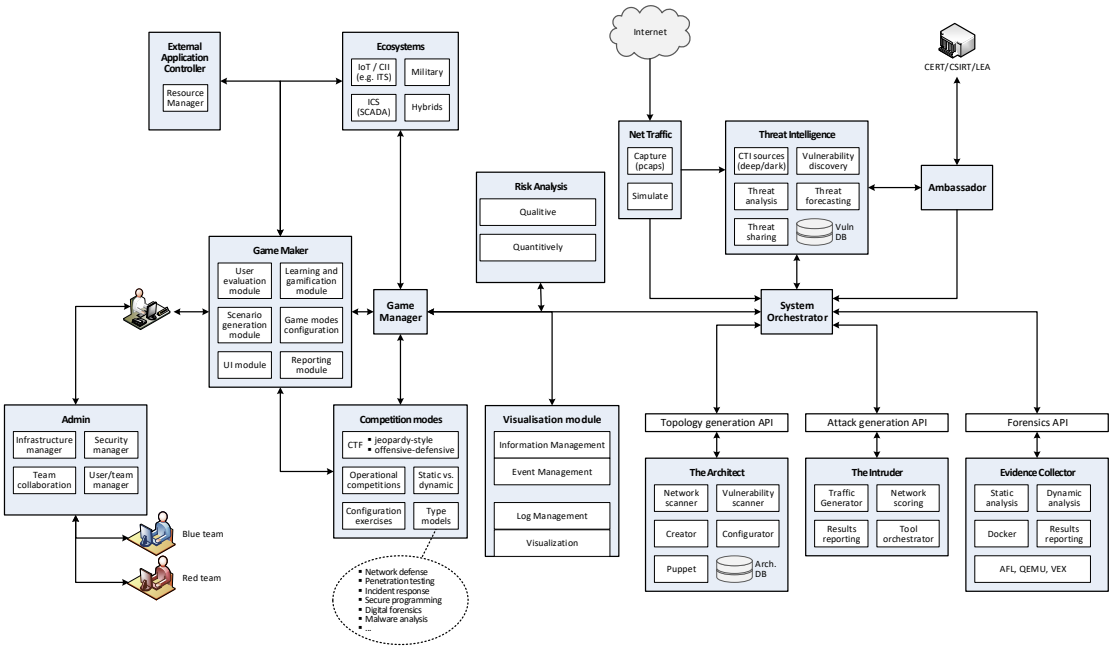

Figure 16: Complete Architecture

5.10 Other representations

As mentioned above, Cyber Ranges can also be categorized by their supporting sector: academic, government or commercial. Furthermore, they can be categorized by how they can be deployed: on premise and as a service. In the following graphs, the reviewed Cyber Ranges are treated as one and the average score is calculated and compared with the proposed Cyber Range. The average score is also calculated per supporting sector, academic, military or commercial, and per deployment method, as a service or on premise, and compared with the proposed one.

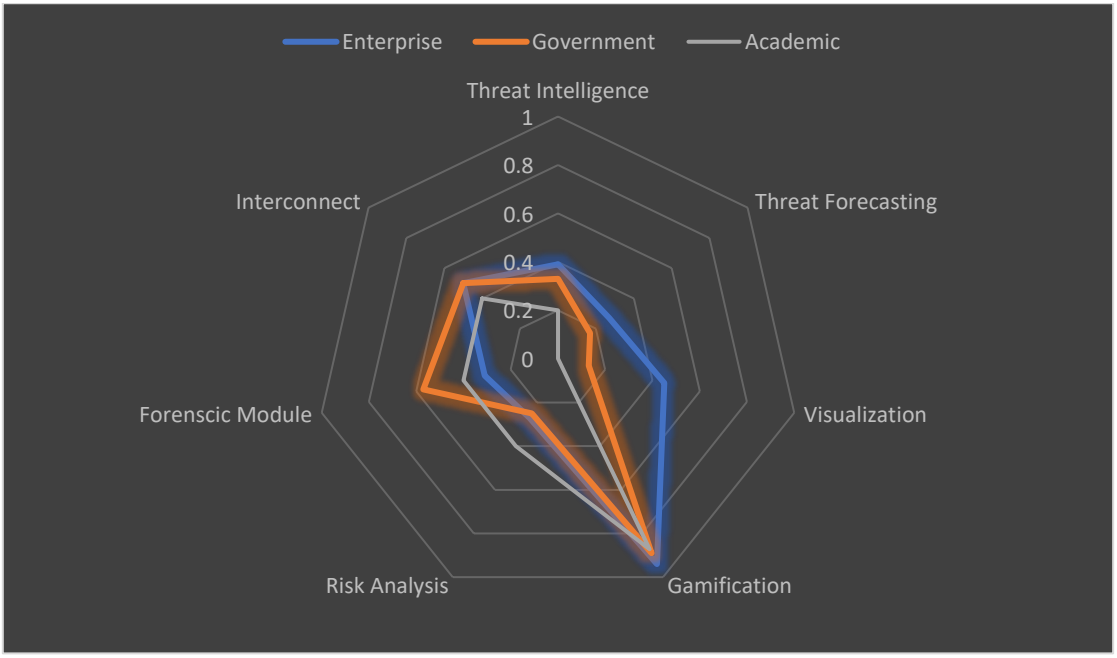

Figure 17: Representation of average per module for Enterprise - Government – Academic

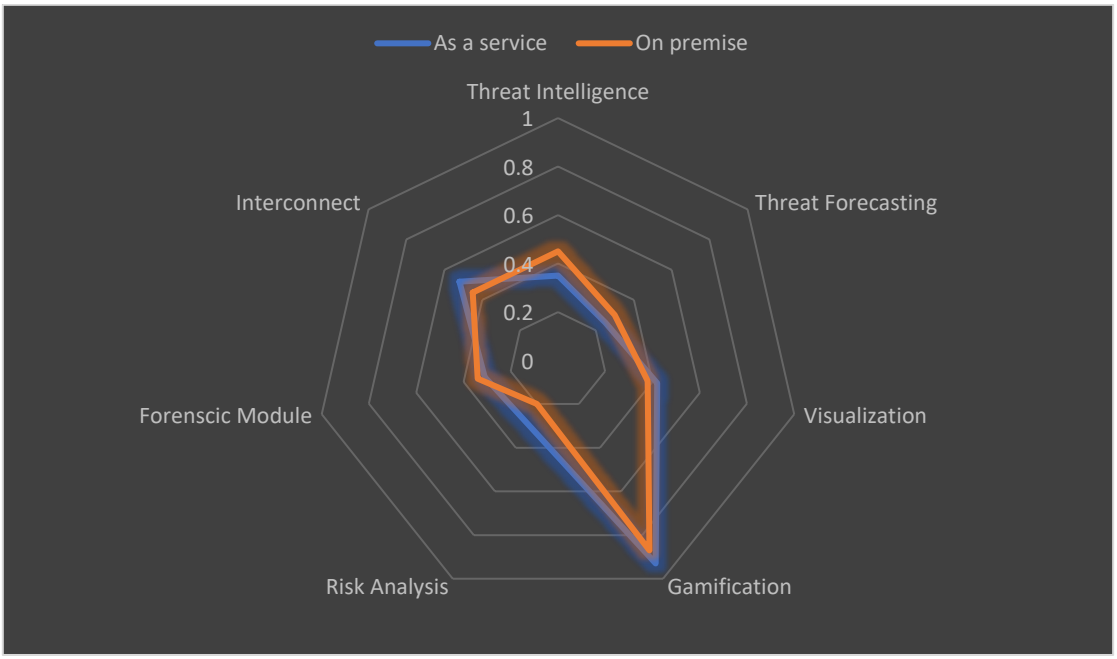

Figure 18: Representation of average per module for deployment method as a service - on premise

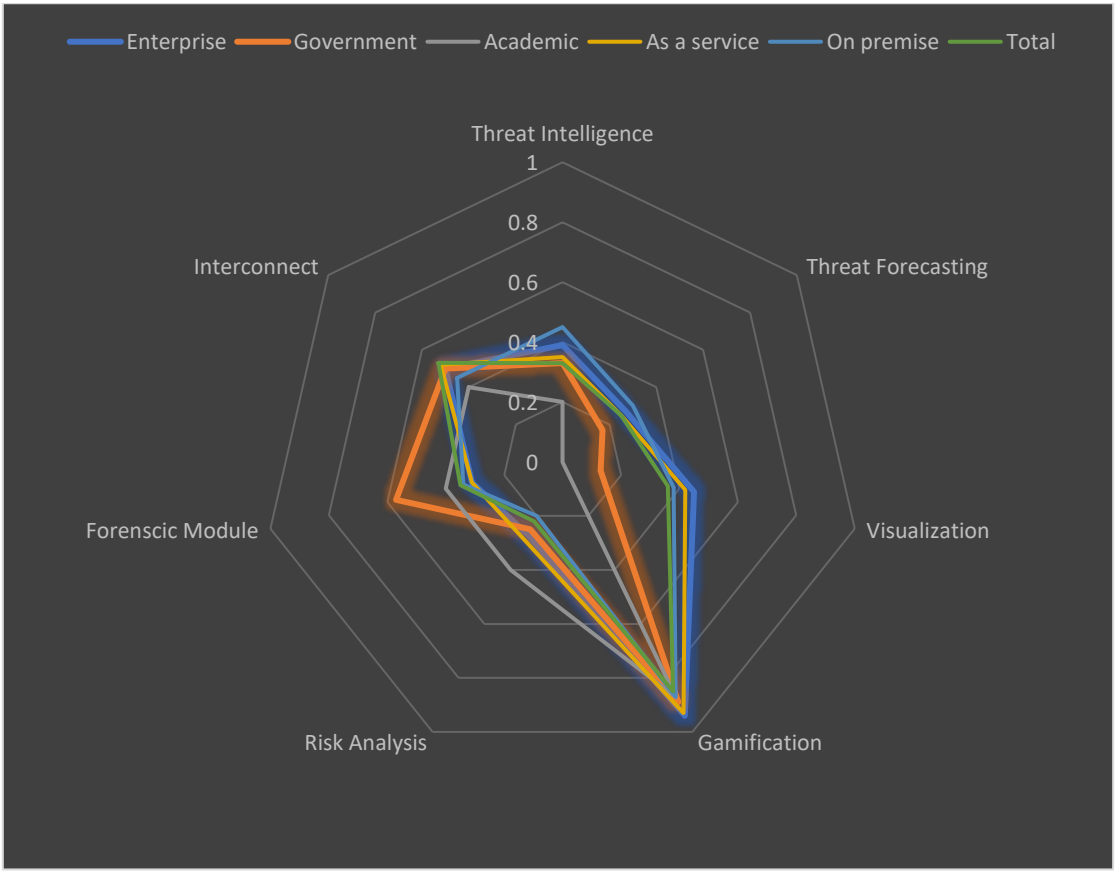

Figure 19: Representation of average per module for enterprise – government – academic - as a service – on premise

Analysing the graphical representations above, regardless of the supporting sector or the deployment method, all of the reviewed Cyber Ranges focus primarily on the gamification module. As for the secondary characteristics, differences are noticed according to the supporting sector: Cyber Ranges whose supporting sector is the government focus more on the forensics module. In addition, Cyber Ranges whose supporting sector is enterprises focus more on visualization.

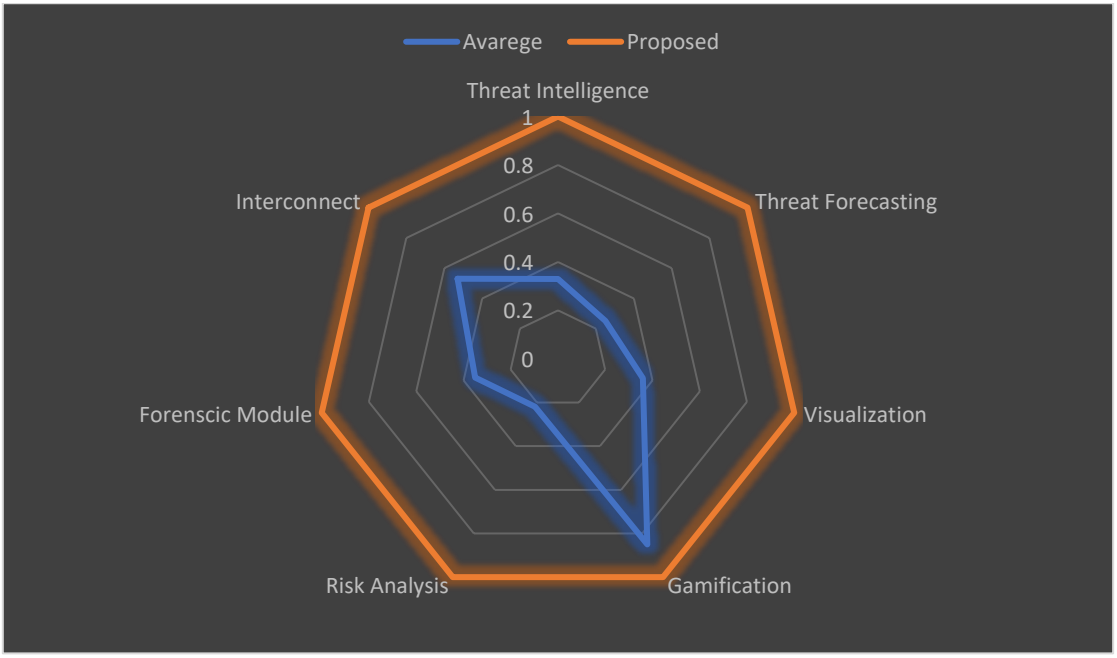

Figure 20: Representation of average per module

6. CONCLUSION

Over the past decade, cyber-attacks have become increasingly sophisticated, stealthy, multi-vector and multistage, which may leverage zero-day exploits and highly creative attack methods. Cyber-security education and training are becoming more and more relevant, as they are the only way to prevent and adequately handle such cyber-breaches. Novel approaches are required, in order to provide organisations, governments and academics with the appropriate situational awareness in relation to cyber-security threats, allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks. Techniques, such as anomaly detection, threat intelligence, visualisation tools, big data analysis, threat analysis, forensic evidence collection, gamification, can be combined in an isolated virtual training environment designed for cyber-security training. Cyber Ranges can provide an environment for continuous training using state-of-the-art methodologies, techniques, a training program covering multiple domains, in order to guide cyber-security experts and professionals in implementing and combining security measures in innovative ways. The proposed architecture aims to train the cyber-security experts in different phases of a large-scale cyber-attack, before and after its occurrence. The proposed modules aim to create a training environment focusing on the prevention, detection, and mitigation of advanced cyber-attacks involving complex networks and hybrid infrastructures. From the demonstrated Cyber Range environments, the majority provide realistic environments emulating complex networks for the cyber-security training of their participants. These systems provide a set of functionalities, such as customized scenarios, virtual environment creation, deployment vulnerability exploitation methods, and the appropriate tools and techniques to mitigate the cyber-threats in the training environment. The common feature of the demonstrated environments is the gamification module, the attack detection and the mitigation methods based on game-centred educational program. Comparing the demonstrated environments with the proposed architecture, the lack of information gathering, sharing and discovery with the use of cyber-threat intelligence, the scarcity of quantitative risk analysis and threat forecasting capabilities can be ascertained. Cyber Range environments should implement a more holistic, adaptable and extendable approach, as the cyber-security landscape evolves across the multiple heterogeneous ecosystems. Cyber-security experts must be able to forecast and detect current and future cyber-threats, to develop skills that will allow them to identify threats and take proper mitigation actions in a fully automated training environment.

ABBREVIATIONS - ACRONYMS

ACT	Attack Countermeasure Tree
AIT	Austrian Institute of Technology
APTs	Advanced persistent threats
ATI	Application and Threat Intelligence
CERTs	Computer emergency response teams
CGC	Cyber grand challenge
CIF	Collective Intelligence Framework
CIIs	Critical information infrastructures
CODE	Cyber Operations, Development and Evaluation
CR	Cyber range
CRITs	Collaborative Research into Threats
CSIRT	Computer security incident response teams
CSR	Cyber Security Range
CTF	Capture the flag
DARPA	Defense advanced research projects agency
DDoS	Distributed denial-of-service attack
DoD	Department of Defense
DoS attacks	Denial-of-service attacks
ENISA	European Union Agency for Network and Information Security
ESA	European Space Agency
EU	European Union

FIRST	Forum of Incident Response and Security Teams
FS-ISAC	Financial Services Information Sharing and Analysis Center
GDP	Gross domestic product
HR	Human resources
IAEA	International Atomic Energy Agency
IasS	Infrastructure as a service
ICS	Industrial control system
ICT	Information and communication technology
IoT	Internet of Things
IT	Information technology
JRSS	Joint Regional Security Stack
LEAs	Law enforcement teams
LMS	Log management
MISP	Malware Information Sharing Platform
MSSPs	Managed security service provider
NCR	National Cyber Range
NHS	National Health Service
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOC	Network operations center
NSA	National Security Agency

OSD	Office of the Secretary of Defense
OT	Operational technology
PaaS	Platform as a service
PLCs	Programmable logic controllers
Saas	Software as a service
SCADA	Supervisory control and data acquisition
SEM	Security Event Management
SIEM	Security information and event management
SIM	Security Information Management
SOC	Security operations center
TRMC	Test Resource Management Center
VMs	Virtual machines
VRF	Virtual routing and forwarding
VTP	Virtual Training Platform

ANNEX I

Web Applications

Web application security is the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application's code. Web application vulnerabilities are typically the result of lack of input/output sanitization, which are often exploited to either manipulate source code or gain unauthorized access.

Theory domains	Lab domains
▪ The secure web application development processes ▪ Risk management for web application security ▪ Architectural risk analysis ▪ Attack patterns and abuse cases ▪ Common design and implementation vulnerabilities ▪ Taxonomy of coding errors ▪ Risk based security testing with threat modeling ▪ Code review with tools ▪ Security testing methods (white / black / gray box testing) ▪ Web application vulnerability assessment ▪ The current threat and vulnerability landscape ▪ Encryption ▪ Operating system security and privacy: Windows, Linux, Mac OS X ▪ Security bugs and vulnerabilities ▪ Reducing threat privilege ▪ Social engineering and social media offence and defense ▪ Security through isolation and compartmentalization ▪ Operating system and application hardening ▪ Malware and hacker hunting on the endpoint ▪ Secure deleting evidence elimination and anti-forensics ▪ Proxies HTTP HTTPS SOCKs and web ▪ Secure Shell	Website penetration testing: ▪ Information gathering o Website enumeration o Understanding DNS o Websites on the same server o Sub domains ▪ File upload, code execution, and file inclusion vulnerabilities o HTTP Requests - GET and POST o Intercepting HTTP requests o Discover and exploit file upload vulnerabilities o Discover and exploit code execution vulnerabilities o Discover and exploit local file inclusion vulnerabilities o Discover and exploit remote file inclusion vulnerabilities o Fixing code execution vulnerabilities o Fixing file upload vulnerabilities ▪ SQL injection vulnerabilities o SQL injections in POST o SQL injections in GET o Bypassing logins using SQL injection vulnerability o Discovering and exploiting blind SQL injections o Enumerate databases o Prevent SQL injection ▪ Cross site scripting vulnerabilities o Discover reflected XSS o Discover stored XSS o Discover Dom based XSS o Exploit and prevent XSS

Theory domains	Lab domains
	▪ Automatically vulnerability discovery using OWASP ZAP o Scanning target website for vulnerabilities o Scan results analysis ▪ Cross-site request forgery (CSRF) vulnerabilities o Manipulating cookies o Discovering CSRF vulnerabilities o Exploiting CSRF vulnerabilities to change administrative password using HTML files o Exploiting CSRF vulnerabilities to change admin password using link o Prevent CSRF vulnerabilities Social engineering: ▪ Information gathering – e.g. website, person, etc. ▪ Generating undetectable backdoors ▪ Spying ▪ Enhancing evil files ▪ Converting evil file to a trojan ▪ Windows evil files ▪ Mac OS X evil files ▪ Linux evil files ▪ Delivery methods ▪ Post exploitation - Meterpreter and Empire

Internet of Things

IoT solutions are notoriously hard to secure, since they combine the security risks of the physical world with those of a cyber-infrastructure. To address such risks, the IoT infrastructure needs to be secured end-to-end, from physical devices to services and data in the cloud.

- Firmware reverse engineering and binary exploitation
  - Reverse engineering firmware binaries
  - Encryption analysis
  - Binary reverse engineering and exploitation
  - Debugging binaries to gain sensitive info
- Hardware-based exploitation
  - Assessing hardware communication protocols such as UART, SPI, I2C etc.
  - JTAG debugging and exploitation
  - Logic sniffing and bus tampering

- Dumping sensitive information and firmware
- Proprietary communication protocol reversing
- Tampering protection mechanisms
- Glitching and side-channel attacks
- Security features included in the hardware

- Web, mobile and cloud vulnerabilities
  - Vulnerabilities in the web applications
  - Mobile apps security issues identification and exploitation (Android and iOS)
  - API-based security issues
  - Cloud-based vulnerabilities

- Radio security analysis
  - Assessment of radio communication protocols
  - Sniffing the radio packets transmitted and received
  - Modifying and replaying the packets for device
  - Jamming-based attacks
  - Radio communication reversing for proprietary protocols
  - Attacking protocol specific vulnerabilities
  - Exploiting communication protocols such as BLE, ZigBee, 6LoWPAN, zWave, LoRa etc.

Software

All challenges will explore the foundations of software security. Software vulnerabilities and attacks that exploit them theoretically and practically are considered important. Common security problems include buffer overflows, integer overflows, injection attacks, such as SQL injection or XSS, and race conditions. Techniques to prevent or detect problems include threat modeling, checklists and coding standards, code reviews, static analysis tools, language-based security, information flow analysis program verification, proof-carrying code, LangSec (language-theoretic security), and security testing incl. fuzzing.

Theory domains	Lab domains
▪ The secure software development processes ▪ Risk management for software security ▪ Architectural risk analysis ▪ Attack patterns and abuse cases ▪ Common design and implementation vulnerabilities ▪ Taxonomy of coding errors ▪ Risk based security testing with threat modeling ▪ Code review with tools ▪ Security testing methods (white / black / gray box testing) ▪ Web application vulnerability assessment	Code review with tools ▪ Code review with RATS and Flawfinder ▪ Code review with Fortify Web application vulnerability assessment ▪ Enumerate web application ▪ Information gathering ▪ Authentication ▪ Access control ▪ SQL injection ▪ Cross-site scripting ▪ Bad passwords,

Theory domains	Lab domains
▪ Fuzz testing	▪ Brute-forcible login ▪ Verbose failure message ▪ Vulnerable transmission of credentials ▪ Fuzz testing Threat analysis and modeling ▪ Security development lifecycle ▪ Identify assets ▪ Create an architecture overview ▪ Decompose the application ▪ Identify the threats ▪ Document the threats ▪ Rate the threats ▪ STRIDE method ▪ DREAD method ▪ Threat analysis with Microsoft *threat analysis and modeling* (TAM) tool ▪ Threat modeling with Microsoft SDL threat modeling tool

Networking

The trainees will be able to identify critical network-centric vulnerabilities that exist in all in-scope networks, systems and hosts.

Theory domains	Lab domains
▪ The current threat and vulnerability landscape ▪ Encryption ▪ Operating system security and privacy: Windows, Linux, Mac OS X ▪ Security bugs and vulnerabilities ▪ Reducing threat privilege ▪ Social engineering and social media offence and defense ▪ Security domains ▪ Security through isolation and compartmentalization ▪ File and disk encryption ▪ Antivirus and end-point protection ▪ Next generation antivirus endpoint protection, detection, response EDR ▪ Endpoint protection technology ▪ Threat detection and monitoring ▪ Operating system and application hardening ▪ Malware and hacker hunting on the endpoint ▪ Secure deleting evidence elimination and anti-forensics ▪ Email security, privacy and anonymity	Network basics ▪ MAC address ▪ Wireless ▪ Wireshark Network penetration testing ▪ Pre-connection attacks ○ Packet sniffing ○ Targeted packet sniffing ○ De authentication attacks ○ Creating fake access points ○ Spoofing MAC address ▪ Gaining access ○ WEP encryption ○ WEP cracking ○ WPA cracking ○ Discovering names of hidden networks ○ Connecting to hidden networks ○ Bypassing MAC filtering ○ Captive portals ○ Securing the network ○ Wireless security

Theory domains	Lab domains
▪ Messengers – security, privacy and anonymity ▪ Virtual private networks VPNs ▪ Tor ▪ VPN and Tor routers ▪ Proxies HTTP HTTPS SOCKs and web ▪ Secure Shell ▪ Bypassing firewalls and deep packet inspection ▪ Chaining nesting privacy ▪ Cellular Networks	▪ Post-connection attacks ○ Information gathering ○ Auto scan and net discover ○ ARP spoofing and sniffing sensitive data ○ Nmap ○ MiTM ARP poisoning and spoofing ○ MiTM bypassing HTTPS ○ MiTM session hijacking ○ MiTM DNS spoofing ○ MiTM keyloggers ○ MiTM code injection ○ MiTM Wireshark ○ Writing custom scripts to execute own attacks ▪ Detection and security ○ Detect ARP poisoning attacks ○ Detect suspicious activities with Wireshark Gaining access ▪ Server-side attacks ○ Information gathering and exploitation ○ Metasploit ○ Code execution ○ Scanning ○ Analyzing results ▪ Client-side attacks ○ Payload creation ○ Backdoor ○ Listening for incoming connections ○ Protection from backdoor ▪ Client-side attacks and SE ○ Discovering emails ○ Discovering social media accounts ○ Analyze information ○ Backdooring any file type ○ Spoofing executables ○ Spoofing emails ○ Hooking methods ○ Creating fake login prompt ○ Trojan detections ▪ Using the above attacks outside the local network ○ Port forward ○ Backdoor outside the network

Theory domains	Lab domains
	Post exploitation ▪ Meterpreter ▪ File systems ▪ Maintaining access ▪ Pivoting ▪ Reverse shell access interaction ▪ Accessing other websites, running shell commands ▪ Bypassing limited privileges and executing shell commands ▪ Uploading files to target web server ▪ Downloading files from target web server ▪ Getting a reverse connection Brute force and dictionary attacks ▪ Brute force & dictionary attacks ▪ Creating a wordlist ▪ Launching a wordlist attack and guessing login password

Cryptography

Data confidentiality, integrity, authentication and non-repudiation are central aspects of modern cryptography that will be considered.

Theory domains	Lab domains
▪ Public and private key encryption ▪ Message authentication codes ▪ Public key infrastructure ▪ Public key infrastructure management ▪ Basic cryptography ▪ Advanced cryptography ▪ Public/private keys ▪ Message digests ▪ Digital signatures ▪ Chains of trust and certificate authorities	▪ Proprietary encryption algorithms ▪ Insecure cipher modes (ECB, CBC, OFB, etc.) ▪ Poor key selection ▪ Insufficient key length ▪ Inappropriate key reuse ▪ Insecure random number generation ▪ Incorrect use of crypto API

Steganography

Steganography, which concerns the secret embedding of data into video, image and audio files, is commonly used in forensic investigations. Main aspects could include:

Theory and lab domains
▪ Data hiding in text ▪ Data hiding in images and videos ▪ Data hiding in audio ▪ Modification of protocol fields ▪ modification of protocol fields or the timing of protocol messages

Theory and lab domains
▪ Lost audio steganography (LACK) ▪ Retransmission steganography (RSTEG)

Malware Analysis

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample, such as a virus, a worm, a Trojan horse, a rootkit or a backdoor on IT systems. Aspects related to static, dynamic and hybrid analysis will be considered.

Theory domains	Lab domains
▪ Malware Analysis Fundamentals ▪ Types of malware, including rootkits, Trojans, and viruses Public key ▪ Types of malware analysis ▪ Introduction to Static analysis ▪ Introduction to dynamic analysis ▪ Introduction to hybrid analysis	▪ Introduction to setting up basic lab for malware analysis ▪ Assembling a toolkit for effective malware analysis ▪ Perform basic dynamic analysis with a sandbox. ▪ Perform basic static analysis with antivirus scanning and strings and examining static properties of suspicious programs ▪ Use IDA Pro to analyze assembly code and malicious Windows programs. ▪ Interacting with malware in a lab to derive additional behavioral characteristics

Reverse Engineering

Reverse engineering is the process of extracting the knowledge or design blueprints from a malicious code or software, while the efforts made in uncovering such a source code are also regarded as reverse engineering. Understanding of disassembler, debugger and decompile will be the main focus.

Theory domains	Lab domains
▪ What Is Reverse Engineering? ▪ Types of Software Reverse Engineering and its applications for e.g. malicious software ▪ Introduction of Reversing Tools ▪ Introduction to Different Reversing Approaches for e.g. ▪ Offline Code Analysis (Dead-Listing) and 110 Live Code Analysis ▪ Introduction to Disassemblers ▪ Introduction to Debuggers ▪ Introduction to Decompilers	▪ Understanding core x86 assembly concepts to perform malicious code analysis ▪ Identifying key assembly logic structures with a disassembler ▪ Following program control flow to understand decision points during execution ▪ Recognizing common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers) ▪ Extending assembly knowledge to include x64 code analysis ▪ How to use key analysis tools like IDA Pro and OllyDbg. ▪ Using Decompilers tools for e.g. System-Monitoring Tools, Patching Tools.

Digital Forensics

Digital forensics is the process of uncovering and interpreting electronic data. Main aspects will include digital forensics related to network, memory and windows fields.

Theory domains	Lab domains
▪ Introduction to Computer Forensics Investigation Process ▪ Understanding Digital Evidence ▪ What is First Responder Procedures? ▪ Understanding Hard Disks and File Systems ▪ Introduction to Windows Forensics ▪ What is Steganography and Image File Forensics? ▪ Introduction to Network Forensics, Investigating Logs and Investigating Network Traffic ▪ Introduction to Mobile Forensics ▪ Introduction of Memory Forensics ▪ How to Investigative Reports? ▪ How to becoming an Expert Witness?	▪ Lab on Digital Forensics - Network Investigation ▪ Lab on D Identify and analyze security attacks, NIDS evidence gathering, Acquisition process, Flow Analysis, Protocol Analysis, Investigating Wireless Attacks Investigating Web Attacks, Analysis, Event Correlation and Aggregation, Tracking Emails and investigating Email Crimes ▪ Lab on Digital Forensics - Windows Investigation ▪ Data Acquisition and Duplication, Recovering Deleted Files and Deleted Partitions, Forensics Investigation using Access Data FTK, Data Acquisition and Duplication, Forensics Investigation Using EnCase, dealing with a turned on/off PC, Gathering essential evidence from Windows log files, RAM, auto-runs, registries etc. Understanding Hard disks and File System. Volatile Information in Windows Forensics, Non-Volatile Information in Windows Forensics. Windows Memory Analysis. Windows Registries. MD5 Calculation, File Signature Analysis. Data Duplication and Acquisition. Investigating Logs and Analyzing Traffic over the Network Cracking Passwords Data Recovery ▪ Lab on Digital Memory Forensics ▪ Memory Forensics Analysis Process for Response and Hunting, Memory Acquisition, Memory Forensics Examinations, Memory Analysis Tools ▪ Lab on Digital Memory Forensics ▪ iPhone Analyzer, BitPim, Mobile Internal Acquisition Tool (MIAT), BitPim, TULP2G, Katana Forensics' Lantern Lite Imager

REFERENCES

[1] European Political Strategy Centre "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level" Issue 24, 8 May 2017; [Online]. Available: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en [Accessed 10/10/18]

[2] Department of Defense Instruction DoDI 8510.01 "Risk Management Framework (RMF) for DoD Information Technology (IT)". 12 March 2014

[3] Global Information Security Workforce Study "2017 Study Results" 2017, [Online]. Available: https://www.isc2.org/Research/Workforce-Study [Accessed 10/10/18].

[4] F Maymir-Ducharme, L Angelelli, D Stapleton - 2015: Cognitive and Autonomic Cyber Defense.

[5] USA Department of Defense "Cybersecurity Test and Evaluation Guidebook", 2015.

[6] NATO Cooperative Cyber Defence Centre of Excellence, "Cyber defence exercises." [Online]. Available: http://ccdcoe.org/event/cyber-defence-exercises.html. [Accessed 15/10/18].

[7] D. Tang, C. Pham, K. Chinen, R. Beuran, "Interactive Cyber Attack Emulation for Facilitating Security Training" Internet Conference (IC 2016), Tokyo, Japan ,11 October 2016

[8] IXIA ,Cyber range: Improving network defense and security readiness. August 2014 Online]. Available: https://www.ixiacom.com [Accessed 21/10/18].

[9] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds". DSTO – Defence Science and Technology Organisation, Technical Report DSTO-GD-0771, 2013.

[10] CTF365, "Capture the flag 365." [Online]. Available: https://ctf365.com [Accessed 9/11/18].

[11] Black T-Shirt Cyber Forensics Challenge [Online]. Available: https://cyberforensicschallenge.com [Accessed 10/11/18].

[12] Bernard Ferguson ; Anne Tall ; Denise Olsen "National Cyber Range Overview" 2014 IEEE Military Communications Conference

[13] S. von Solms ; S. W. Peach "The design and implementation of a network simulation platform" 2013 International Conference on Adaptive Science and Technology.

[14] Vicente Pastor ; Gabriel Díaz ; Manuel Castro "State-of-the-art simulation systems for information security education, training and awareness" IEEE EDUCON 2010 Conference

[15] Jan Vykopal ; Martin Vizvary ; Radek Oslejsek ; Pavel Celeda ; Daniel Tovarnak "KYPO Cyber Range: Design and Use Cases"

[16] Jan Vykopal ; Martin Vizvary ; Radek Oslejsek ; Pavel Celeda ; Daniel Tovarnak "Lessons learned from complex hands-on defence exercises in a cyber range" 2017 IEEE Frontiers in Education Conference (FIE)

[17] Virginia Cyber Range [Online]. Available: https://virginiacyberrange.org [Accessed 15/11/18].

[18] CYBERBIT [Online]. Available: https://www.cyberbit.com [Accessed 15/11/18].

[19] Info security [Online]. Available: https://www.infosecurityeurope.com [Accessed 15/11/18].

[20] Raytheon [Online]. Available: https://www.raytheon.com [Accessed 15/11/18].

[21] Cisco Cyber Range [Online]. Available: https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf [Accessed 10/1/19].

[22] European Space Agency [Online]. Available: https://www.esa.int/About_Us/Welcome_to_ESA/ESEC [Accessed 10/1/19].

[23] Cybexer technologies [Online]. Available: https://cybexer.com/ [Accessed 7/2/19].

[24] IBM Cyber Range [Online]. Available: https://www.ibm.com/security/services/managed-security-services/security-operations-centers [Accessed 10/1/19].

[25] Palo Alto Networks Cyber Range [Online]. Available: https://www.paloaltonetworks.com/resources/techbriefs/cyber-range [Accessed 6/1/19].

[26] Silensec Cyber Range [Online]. Available: https://www.silensec.com [Accessed 2/1/19].

[27] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" August 2017.

[28] Austrian Institute of Technology Cyber Range [Online]. Available: https://www.ait.ac.at/en/ [Accessed 10/1/19].

[29] Splunk [Online]. Available: https://www.splunk.com [Accessed 5/12/18].

[30] Quali [Online]. Available: https://www.quali.com [Accessed 7/12/18].

[31] Fortinet [Online]. Available: https://www.fortinet.com [Accessed 22/12/18].
[32] IXIA "Boosting Singapore'sCyber Security Skills" January 2018.
[33] Sypris electronics cyber range [Online]. Available: https://www.sypriselectronics.com/information-security/cyber-security-solutions/cyber-range [Accessed 25/12/18].
[34] NEC Cyber Range [Online]. Available: https://www.nec.com/en/global/solutions/cybersecurity/advantage/index.html [Accessed 3/1/19].
[35] Georgia Cyber Institute [Online]. Available: https://cyber.augusta.edu/georgia [Accessed 4/1/19].
[36] Horizon 2020 Work Programme 2018-2020 "Cyber-security preparedness - cyber range, simulation and economics" [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ds01-2018
[37] FireEye "Advanced Targeted Attacks How to Protect Against the Next Generation of Cyber Attacks" 2012
[38] Maochao Xu ; Kristin M. Schweitzer ; Raymond M. Bateman ; Shouhuai Xu "Modeling and Predicting Cyber Hacking Breaches" IEEE Transactions on Information Forensics and Security (Volume: 13 , Issue: 11 , Nov. 2018)
[39] Shane Powell "Cyber Effects Prediction" *BlackHat-DC-2010*
[40] John R. Goodall ; Daniel R. Tesone "Visual Analytics for Network Flow Analysis" 2009 Cybersecurity Applications & Technology Conference for Homeland Security
[41] National Institute of Standards and Technology "Guide for ConductingRisk Assessments" NIST Special Publication 800-30 Revision 1
[42] CTF TIME DEF CON CTF Qualifier 2018 [Online]. Available: https://ctftime.org/event/608 [Accessed 10/1/19].
[43] Rahul Neware ; Amreen Khan "Cloud Computing Digital Forensic challenges" 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)
[44] Wiem Tounsi , Helmi Rai "A survey on technical threat intelligence in the age of sophisticated cyber attacks" April 2017
[45] MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing [Online]. Available: http://www.misp-project.org [Accessed 7/2/19].
[46] Collaborative Research Into Threats [Online]. Available: https://crits.github.io [Accessed 10/1/19].
[47] Financial Services Information Sharing and Analysis Center [Online]. Available: https://www.fsisac.com [Accessed 10/1/19].
[48] Collective Intelligence Framework [Online]. Available: https://github.com/csirtgadgets/massive-octo-spice/wiki/Introduction [Accessed 10/1/19].
[49] Open Source Threat Intelligence Gathering and Processing Framework [Online]. Available: https://github.com/ciscocsirt/GOSINT [Accessed 9/11/18].
[50] MineMeld indicator processing framework [Online]. Available: https://github.com/PaloAltoNetworks/minemeld [Accessed 8/11/18].
[51] Cisco [Online]. Available: https://www.cisco.com/c/en/us/products/security/security-reports.html [Accessed 10/1/19].
[52] Cambridge Intelligence [Online]. Available: https://cambridge-intelligence.com/use-cases-graph-visualization-cyber-security [Accessed 10/1/19].
[53] AlienVault OSSIM [Online]. Available: https://www.alienvault.com/products/ossim [Accessed 9/11/18].
[54] Elastic [Online]. Available: https://www.elastic.co [Accessed 3/1/19].
[55] Lihua Hao ; Christopher G. Healey ; Steve E. Hutchinson "Ensemble visualization for cyber situation awareness of network security data" 2015 IEEE Symposium on Visualization for Cyber Security (VizSec)
[56] Deterding Sebastian,Dixon Dan, Khaled Rilla,Nacke, Lennart "From Game Design Elements to Gamefulness: Defining Gamification" September 2018
[57] Harshal Tupsamudre, Rahul Wasnik,Shubhankar Biswas,Sankalp Pandit,Sukanya Vaddepalli, Aishwarya Shinde, C. J. Gokul, Vijayanand Banahatti, Sachin Lodha "GAP: A Game for Improving Awareness About Passwords" October 2018
[58] The Necromancer Author: Xerubus [Online]. Available: https://www.vulnhub.com/entry/the-necromancer-1,154 [Accessed 4/1/19].
[59] Cryptomancer RPG [Online]. Available: http://cryptorpg.com [Accessed 4/1/19].

[60] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education", in proc. *2013 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 915-928, Nov. 2013.
[61] Mikel Salazar ; José Gaviria ; Carlos Laorden ; Pablo G. Bringas "Enhancing cybersecurity learning through an augmented reality-based serious game" 2013 IEEE Global Engineering Education Conference (EDUCON)
[62] National Institute of Standards and Technology "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" 2017
[63] National CyberWatch Center "2017-2018 Annual Report – National Cyber Watch Centre" [Online]. Available: https://www.nationalcyberwatch.org/ncw-content/uploads/2018/03/2017-18_NCC_Annual_Report_Web.pdf [Accessed 5/1/19].
[64] S. von Solms ; S. W. Peach "The design and implementation of a network simulation platform" 2013 International Conference on Adaptive Science and Technology
[65] Georgiana Subaşu ; Livia Roşu ; Ion Bădoi "Modeling and simulation architecture for training in cyber defence education" 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)
[66] National Institute of Standards and Technology "NIST Guide for Conducting Risk Assessments" NIST Special Publication 800-30Revision 1
[67] Philip L. Campbell, Jason E. Stamp "A Classification Scheme for Risk Assessment Methods" SANDIA REPORT SAND2004-4233 August 2004
[68] SC Patel, JH Graham, PAS Ralston "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements" June 2008
[69] Yulia Cherdantseva , Pete Burnap , Andrew Blyth , Peter Eden , Kevin Jones, Hugh Soulsby, Kristan Stoddar "A review of cyber security risk assessment methods for SCADA systems" May 2015
[70] Eric J. Byres , Matthew Franz , Darrin Miller "The use of attack trees in assessing vulnerabilities in scada systems" in IEEE Conf. International Infrastructure Survivability Workshop (IISW '04). Institute for Electrical and Electronics Engineers.
[71] Arpan Roy ,Dong Seong Kim, Kishor S. Trivedi "Cyber security analysis using attack countermeasure trees"
[72] Daniel DiMase , Zachary A. Collier , Kenneth Heffner, Igor Linkov "Systems engineering framework for cyber physical security" February 2015
[73] Yiling Zheng ; Song Zheng "Cyber Security Risk Assessment for Industrial Automation Platform" 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)
[74] National Institute of Standards and Technology "Notes Guide to Integrating Forensic Techniques into Incident Response" NIST SP800-86
[75] Arnoud Goudbeek, Kim-Kwang Raymond Choo, Nhien-An Le-Khac "A Forensic Investigation Framework for Smart Home Environment" Conference: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[76] Ana Nieto "An Overview of Proactive Forensic Solutions and its Applicability to 5G" 2018 IEEE 5G World Forum (5GWF)
[77] T Min, X Jianying, Y Tao "Research on Electronic Data Forensics Model under Cloud Computing" 2018 International Conference on Smart Grid and Electrical Automation (ICSGEA)
[78] Moloch [Online]. Available: https://github.com/aol/moloch#usage [Accessed 6/1/19].
[79] Security Onion [Online]. Available: https://github.com/Security-Onion-Solutions/security-onion [Accessed 10/1/19].
[80] OSSEC [Online]. Available: https://github.com/ossec/ossec-hids [Accessed 7/1/19].