



Cyber range design framework for cyber security education and training

M. N. Katsantonis² · A. Manikas² · I. Mavridis² · D. Gritzalis¹

© The Author(s) 2023

Abstract

The need for effective training of cyber security personnel working in critical infrastructures and in the corporate has brought attention to the evolution of Cyber Ranges (CRs) as learning and training tools. Although CRs have been organized for many years, there is a lack of standards and common methodologies that facilitate their development and optimize their effectiveness. Aiming at strengthening cyber security education and research that utilize well designed CRs, we first analyze the CRs domain to identify key characteristics, strengths and fundamental weaknesses, and based on these outcomes we propose the Cyber Range Design Framework (CRDF), which includes the CR Architecture and the CR Life-Cycle. The CR Architecture presents the main components of CRDF compliant CRs, whereas the CR Life-Cycle presents the development phases of such approaches and the activities these phases embrace. CRDF builds on the Conceptual Framework for eLearning and Training (COFELET) and on the Exercise Life-Cycle. COFELET is particularly elaborated for the development of cyber security educational approaches, by adopting its design considerations that were based on widely adopted educational theories and approaches (e.g., scenario-based, reuse of elements). CRDF envisages the elaboration of CRs which optimize their impact, mitigate their weaknesses, and minimize their preparation and running costs. Under this prism, a preliminary appreciation of the CRDF approaches effectiveness is presented along with the expected outcomes of such approaches.

Keywords Cyber range · CRDF · Design framework · Architecture · Life cycle · COFELET

1 Introduction

The digitization of our world has highlighted cyber security as a key priority for the government, the corporate sector and for individuals. As the dependence on information and communication technologies grows, cyber security threats and attacks by cybercriminals and cyberwarriors (i.e., attackers acting on behalf of other countries) increase. According

to McAfee's report "The Hidden Costs of Cybercrime" [1] the monetary cost of cybercrime, carried out globally, is estimated at approximately 945 billion dollars. The global economic loss caused by cybercrime approaches 1 trillion dollars which exceeds 1% of the global economy [1]. This amount is expected to reach 10.5 trillion dollars annually until 2025 [2]. During 2021 the cybersecurity workforce of Europe and the America has increased by 30%, but the global demand for cybersecurity professionals continues to outpace supply—resulting in the cybersecurity workforce gap [3].

A key factor in the ongoing cyber warfare is the availability and readiness of competent cyber security personnel, the frontline of defense against cybercrime. Through more effective education and training, the cyber security workforce can be increased, whereas the knowledge and skills of the cyber security personnel working in companies, agencies and organizations can be enhanced. Nevertheless, an important condition for the society and economy broadly resistant to cyber threats is the raise of cyber security awareness of the cyberspace end users.

✉ D. Gritzalis
dgrit@aueb.gr

M. N. Katsantonis
mkatsantonis@uom.edu.gr

A. Manikas
manikas@uom.edu.gr

I. Mavridis
mavridis@uom.edu.gr

¹ Department of Informatics, Athens University of Economics and Business, 11253 Athens, Greece

² Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece

In nowadays, cyber security education heavily relies on traditional teaching methods, including lectures, workshops, seminars, and labs [4]. Cyber Ranges (CRs) are an important element of the cybersecurity education and training, as they provide a platform for conducting cyber security exercises, tests, and experiments through which participants can be trained and qualified by exercising their knowledge and skills, and by performing hands-on activities [5]. Moreover, it is evident that CRs have the potential to effectively contribute to the addressing of the global skills shortage, and the updating of knowledge in the field of cyber security [6]. However, several limitations constrain the CRs' potential mainly regarding the organizational issues such as the high demands of the organization and execution of CRs, and the lack of skilled personnel who will participate in CRs (e.g., attackers, defenders). Although various CRs have been organized for many years there is a lack of standards and common methodologies to facilitate their development and confront their limitations and challenges.

The aim of this study is to effectively contribute to the strengthening of cyber security approaches, which utilize CRs, through the proposal of the Cyber Range Design Framework (CRDF) for the development of cyber security education, training and assessment approaches. CRDF can be utilized as a means of improving the CRs potential and confronting the current CRs' weaknesses. CRDF includes the CR Architecture which proposes the main parts a CRDF compliant CR (CRDF approach) has to embrace, the functions it has to perform, and the manner that it can be organized. The CR Life-Cycle suggests the phases of development of a CRDF approach, and the activities the phases must unfold. CRDF is based on the Conceptual Framework for eLearning and Training (COFELET) and the Exercise Life-Cycle [4], as it contemplates the COFELET's design considerations [7,8], it embodies the COFELET ontology elements (e.g., tasks, conditions, scenarios, steps, SEFs) [8,9], and it adapts phases of the Exercise Life-Cycle. COFELET's design considerations are the foundation of the CRDF approaches on the appropriate learning strategies (i.e., modern and traditional); the facilitation of elements' reuse; the emphasis put on the performance of dynamic assessment, the adaptability to the learners' needs and capabilities; the provision of real-time feedback; the inclusion of objects and scenarios repositories; the definition of roles and target knowledge, skills and abilities (KSAs) for the learners; and the conformance with cyber security standards and models. Through its compliance with the COFELET framework, CRDF assimilates modern educational approaches, simulations, visualizations and gamification elements, and it specifies the key elements that have to be included to support these features, and the manner these elements have to be organized. The presented study was initiated with the analysis of the state of the art CRs, in order to identify their key characteristics, examine their strengths

and weaknesses, and consider them for the elaboration of the proposed framework.

The remainder of this paper is organized as follows: Sect. 2 presents the works related to this study; Sect. 3 provides an analysis of the CR domain resulting in the specification of current CRs' characteristics (e.g., types, categories, technologies) and weaknesses; Sect. 4 presents the proposed framework which is composed of the CR Architecture and the CR Life-Cycle; Sect. 5 presents a preliminary evaluation of CRDF; Sect. 6 discusses the expected outcomes of the proposed framework, and the last section concludes the paper.

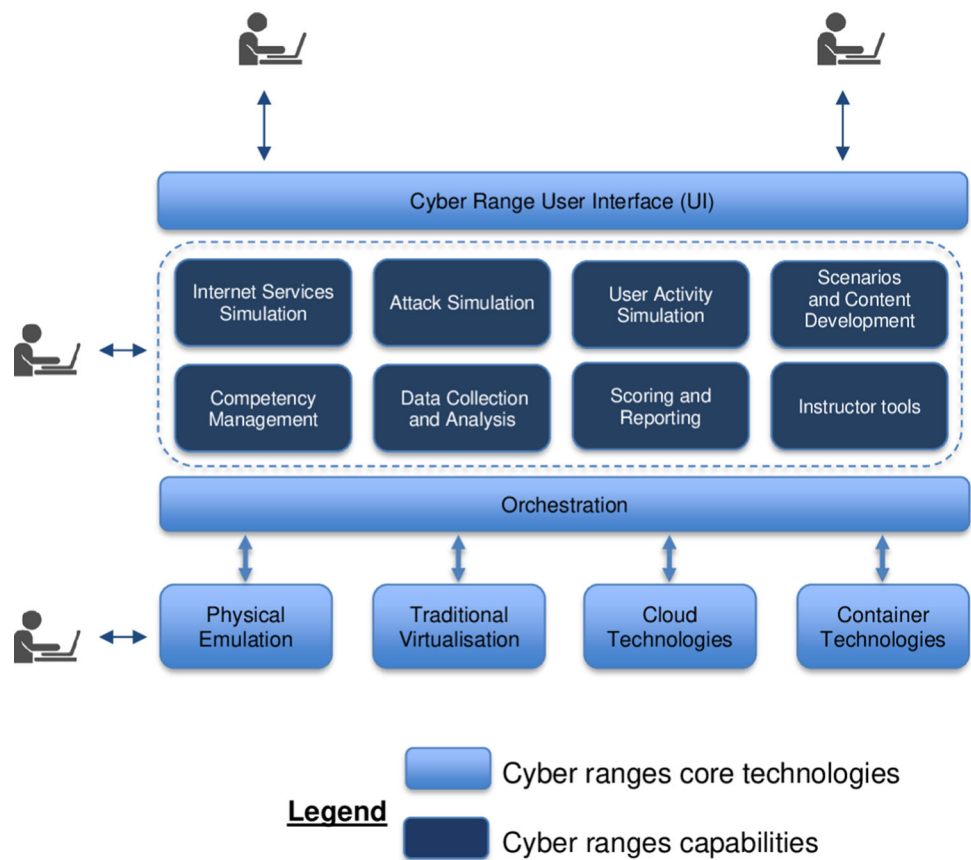
2 Related work

Several studies explore the CR domain including use cases, literature reviews, CR capabilities and weaknesses. The National Institute of Standards and Technology (NIST) in [5] provides a guide for CRs, which defines the term "cyber range", explores the CR use cases and presents the CR target groups, capabilities and a list of criteria for CR type selection. NIST defines CRs as "interactive, simulated platforms and representations of networks, systems, tools, and applications" [5], which can be considered as limiting. According to NIST, a CR can provide an authentic, legal and safe environment for: implementation of cyber security courses, continuing education and training, testing of new cyber security products and settings, and testing of knowledge and skills of individuals. However, NIST's definition of CRs is considered limited, as it emphasizes on the technical characteristics of CRs.

The European Cyber Security Organization (ECSO) in [10] provides an overview of CRs and associated use cases, focusing on the functionalities and capabilities of CRs, the utilized technologies for the development of CRs, and the limitations of the current CR implementations. ECSO claims that the NIST's definition does not refer to the operations and the services the CRs provide, and that it defines CRs more as platforms [11] rather than simulation environments. ECSO defines a CR as "a platform for the development, delivery and use of interactive simulation environments". According to ECSO, a CR combines a set of core technologies for the implementation of the simulation environment, and additional components for the development of particular cyber range use cases. ECSO also proposes an abstracted architecture, as depicted in Fig. 1, which focuses on core technologies and the capabilities of CRs.

In contrast with the NIST's definition, ECSO adopts a wider meaning by characterizing CRs by the "different types of users" and the "different purposes" they are used for, and proposes a set of architectural components, embedded functionalities, and underpinning technologies. However, ECSO

Fig. 1 Sample architectural components of a cyber range [10]



does not present the manner the proposed components can be organized and interconnected to assist the design of CRs. Besides ECSO does not present how each of the proposed components contributes to the desired capabilities and functionalities presented in their overview. Ukwantu et al. [12] extend ECSO's architecture and provide details on the manner some of the proposed components of CRs operate, as a result of a literature review, which examines the existing CRs since 2015, and classifies them in various manners according to their application (e.g., military, academic), type (e.g., private, federated) and implementation method (e.g., emulation or simulation).

Yamin et al. [13] conducted a literature review on CRs and testbeds, and they defined a taxonomy which includes their capabilities and functions. The taxonomy contains 48 elements, which are classified with respect to the general concepts: Monitoring, Learning, Management, Teaming, Environment, and Scenario. Likewise, the literature review in [12], presents a different CR taxonomy, which includes 107 elements classified into the general concepts: Teaming, Types, Econometrics, Monitoring, Management, Test-beds, Recovery Attack type, and Scenarios. Both taxonomies classify CRs and aid the analysis and comprehension of CRs' elements. However, as they include a high level of abstraction, they focus mostly on high-level aspects of CRs, which

do not provide guidance for the design of low-level elements of CRs. For example, the learning and education elements of the taxonomies do not define the low-level pedagogical elements of CRs such as the applied teaching strategy, the learning objectives, the teaching contents and the scaffolding and assessment strategies. Moreover, the high level of abstraction does not help at understanding the manner the CR elements are associated with the CR requirements and capabilities, and thus, assumptions cannot be made on the CR element's potential to satisfy the desired requirements and improve CRs' effectiveness.

3 Cyber range analysis

In this section, the conducted analysis of the cyber range domain is presented. The presented analysis has two objectives: (1) to identify the quality characteristics of the state of the art in the CRs domain, (2) to reveal the weaknesses that limit the effectiveness in developing and operating CRs. In the beginning of the section, the methodology followed for the literature search and the selection and examination of CRs, is described.

3.1 Methodology

In the initial phase of the presented study a clear definition of the research questions, which guide the literature search, was made. The following questions were formulated:

- Which are the existing frameworks for the design and development of a CR?
- Which components does a CR architecture include?
- What are the main categories and common characteristics of CRs?
- Is the education and training process provided through CRs, based on pedagogical methods and strategies?

In the second stage the selection of the digital databases in which the search would be carried out was made. The search was initially performed in the databases of Science Direct, Springer, MDPI, IEEE Explore, Wiley, Research Gate as well as Google Scholar. In addition to the above, the search was extended also to reports and deliverables of related research and innovation projects and CR official websites.

The next stage involved defining the keywords and the inclusion and exclusion criteria of the search results. The search focused on the most recent publications, with an emphasis on those of the last 11 years, and those related to the initial research questions. An example of the keywords used for the conducted search is: (“Cyber Ranges” OR “Test Beds”) AND (“Architecture” OR “Framework” OR “Education” OR “Training” OR “Testing”)

The search yielded 93 publications that provided information on 40 CRs. The results were filtered and grouped according to the characteristics of the CRs such as the CR sector (i.e., Academic, Government, Private, Industrial, Research, Commercial) and the CR types (e.g., Federal, Public, Private). Additional grouping had to be done regarding the characteristics of the participants and the aim of the CR (i.e., Certification, Educational, Training, Testing) and after the final filtering the remaining CRs were 27, as the information collected was sufficient and aligned with the original search questions.

At the same time, several interviews were conducted with cyber security experts working for the government and the military, including the Military Computer Incident Response Center (MCIRC) and the Hellenic Computer Security Incident Response Team (CSIRT), who have long experience in participating in CRs as players, instructors and organizers. The interviews with CR experts aided in the comprehension of the most important capabilities of current state of the art in the CR domain (e.g., NATO Cyber Range) and in identifying the key requirements of CRs.

In the next phase of this study, each of the selected papers was examined and multiple characteristics of CRs were derived in the form of common and key characteristics, and

weaknesses in the CR domain. The identified characteristics were recorded in a topic map and described in more detail in the next subsection.

3.2 Cyber range characteristics

Figure 2 depicts the proposed topic map of CRs identified in the selected paradigms of CRs found in the literature. Topic Maps [14] are a standardized manner [15] to represent knowledge, and they consist of topics, associations, and occurrences. CR characteristics were recorded as topics (represented in Fig. 2 by ellipses), whereas the results of the search were recorded as the topic map’s occurrences represented by numeric captions in the topics. The recorded topics were correlated and merged gradually and they were analyzed according to their subject (e.g., utilized technologies, type, pedagogical elements). Then, they were grouped into categories, and finally, the relationships between the related topics were defined as associations of the topic map. The labels connected with the associations (the captions in brackets) denote the roles of the topics in these associations. Although occurrences in topic maps are associated with the resources containing information about the topics, in the proposed topic map for readability purposes the occurrences are represented by numbers in the topics, to denote the number of the selected CRs embracing the characteristics of the CRs.

The characteristics of CRs depicted in the proposed topic map are presented in the remainder of this section.

3.2.1 Types

The type of a CR is determined by its aims and objectives [16], the roles participants adopt while using it, and the characteristics of the participants. A CR may support one or more of the following types:

- Educational CRs are used for cybersecurity education and training. They have the form of an organized learning environment aiming at teaching various cybersecurity subjects and offering opportunities for hands-on practice in cyber security.
- Certification CRs are used for assessing and certifying the degree that distinct cybersecurity knowledge and skills are possessed by the participants. They often take the form of competitions, e.g., Cyber Defense Exercises (CDX), Capture the Flag (CTF).
- Test CRs are used for research and development purposes, e.g., to try out cybersecurity products (cybersecurity-related technologies, tools, and measures) and assess their effectiveness.

Educational CRs and certification CRs involve instructors, cybersecurity experts, and learners or trainees attending

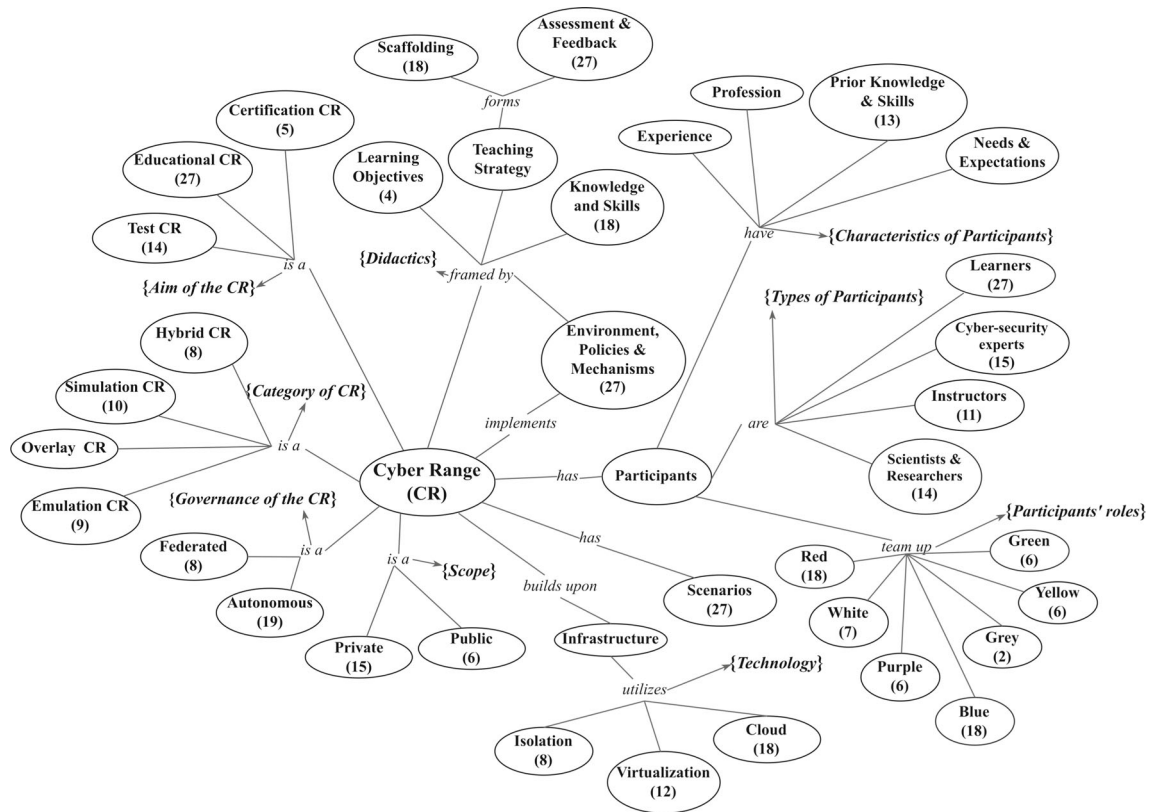


Fig. 2 Topic map of cyber range characteristics

cybersecurity courses or programs. The role of the instructors is to monitor the learners’ efforts and interfere when learners are puzzled, while the role of the cyber security experts is to perform technical tasks such as constructing and configuring the CR’s infrastructure, debugging and injecting vulnerabilities in the CR infrastructure. Participants may adopt different roles, work individually or collaboratively. The most common roles in CRs are of the blue and red team. The blue team members either assume the role of the cyber security personnel (defenders) of a system protecting it from cyber-attacks or the role of forensics investigators investigating a cyber-attack and its consequences [17]. The red team members perform cyber-attacks by assuming the role of attackers who discover vulnerabilities. In CRs where trainees adopt the role of the blue team, the attacks are carried out by a red team of cyber security experts, or they are executed in an automated manner.

CRs often take the form of competitions such as Capture the Flag (CTF) exercises and Cyber Defense Exercises (CDX). CTFs competitions focus on attack techniques helping participants to develop adversarial thinking and preparing them to better deal with possible cyber-attack activities. On the other hand, participants of CDX competitions are mainly trained in defensive techniques which help them anticipate possible cyber-attacks [4]. CTF competitions overlap with

CRs, as they have similarities in the manner knowledge is disseminated, skills are built (capacity building) and evaluated, and in the way they are utilized as a learning tool in cybersecurity education [18]. There are several CRs through which CTF competitions are organized and conducted, such as the SPIDER CR, US CR, AIRBUS CR, AIT CR and the University of Delaware CR. The utilization of CRs in CTF competitions could enhance the authenticity of CTFs [19] and change the way they are organized, providing the opportunity to organize similar events on a larger scale [10,20] recognizes CRs as cyber security and cyber warfare training environments, considering them ideal for conducting CTF competitions.

CRs may also be distinguished according to their governance as:

- Autonomous CRs, which operate independently, without the need to communicate or to be integrated into other CRs.
- Federated CRs, which consist of interconnected autonomous CRs which involve reduced costs, as the organizers share the costs, and the information and human resources required to prepare and run the CRs [21].

According to the Cambridge dictionary [22], a federation is: “a group of organizations, countries, regions, etc. that have joined together to form a larger organization or government”. In information technology, a federation is a group of computer or network providers that agree on specific operating standards. The operational standards of CRs include a scenario description language, a description of the CR capabilities, and the provision of CR services within the federation [10].

3.2.2 Categories

Davis and Magrath [18] conducted an extensive review of approximately 30 unclassified CRs from the academic, commercial, and military domains and they [23] grouped CR platforms into three main categories according to their technology aspects:

- Simulation CRs, which use software tools to form the network of the CR, and thus no physical network equipment is required. Simulation CRs can be scalable, flexible, and cost-effective. However, they have limited fidelity compared to the overlay CRs [5,18,23].
- Overlay CRs, which use physical network equipment and operate on physical computing devices. Overlay CRs provide a higher level of fidelity compared to simulation CRs, but they may have issues regarding hardware cost and network infrastructure breaching [5].
- Emulation CRs, which replicate the physical infrastructure of specific business networks. They involve a high degree of fidelity and realism, and they demonstrate repeatability of execution. They are not as scalable as simulation CRs, and they generally have a higher cost. The high costs are reduced by the sharing of resources and the use of virtualization technologies [5,18,23].

Emulation and simulation CRs are the most common categories of CRs; emulation CRs are effective and realistic approaches, although the hybrid CRs are gaining more and more interest. Priyadarshini [20], analyzed several CRs and proposed four CR categorizations according to:

1. The type of the underlying infrastructure (i.e., public, private, or federated).
2. The utilization of cloud computing technologies, and the inclusion of a virtual private network (VPN).
3. The characteristics of the participants (e.g., students, professionals, trainees) or the supported teams (i.e., red, blue, purple, green, white, yellow, gray).
4. The utilization of virtualization technologies (e.g., the use of virtual machines) or the combination of virtualization and isolation technologies (e.g., sandbox mechanisms). Although both VMs and sandboxes provide isolation,

VMs require more computing resources and they provide full isolation, unlike sandboxes that provide flexible isolation with less costs in terms of computing resources. Finally, VMs are more convenient for malware testing than sandboxes, which is the reason that most CRs are not entirely sandbox-based.

ECISO [10] identifies two categories of CRs, based on the development technology:

1. Conventional CRs are based on virtualization technologies through the employment of virtual machines utilizing hypervisors or containers or a combination of these two software technologies. A VM can simulate the behavior of any computing device. Hypervisors help at the management of the CR’s physical resources and the prevention of conflicts between VMs, whereas containers share the operating system of a VM and, thus multiple containers can be included in a single VM. Building a CR on conventional virtualization offers the advantages of a high degree of flexibility and control over the data and the information being processed by the CR. On the other hand, utilizing hypervisors and containers have limitations because they include restrained orchestration capabilities and increased costs (e.g., the annual cost for the user licenses). The main advantage of containers is their economic performance due to their orchestration and communication capabilities. However, incorrect settings of a container may have a negative impact on data security or even compromise adjacent containers.
2. Cloud CRs are based on cloud computing technologies and on hypervisor software, which manages the available physical computing resources and offers high efficiency and reduces cost. In addition, cloud CRs can also implement virtualization using containers. Cloud computing is the most appropriate approach for CR design, as apart from the aforementioned advantages they can offer increased scalability and orchestration, and dynamic configuration support. Cloud CRs based on cloud computing can be further categorized into private, public or hybrid, as is the case with any other business application developed with cloud computing technologies.

3.2.3 Didactics

The didactics characteristic contains notions associated with the educational or training program developed on the basis of a CR, and it includes the following features:

- Learning objectives, which are brief descriptions of the knowledge and skills that learners are expected to acquire and practice during CR.

- Theoretical background, which includes specific teaching materials (e.g., text, videos) that learners need to assimilate to be able to perform the activities of a CR project.
- Teaching strategy, which determines the educational methodology applied to aid participants achieve the learning objectives.
- Scaffolding, which defines the manner the participants' efforts are supported in performing the CR activities and fulfilling the learning objectives.
- Environment, where the CR project is performed such as a laboratory with the participants' physical attendance or a cloud infrastructure which participants access remotely.
- Assessment strategy, which determines the plan followed for the evaluation of the learner's performance. Learners' efforts are evaluated both during the CR project (formative assessment) and after the end of the CR project (summative assessment). The assessment strategy defines the manner learners' efforts are measured (grading) and the manner feedback is provided to the participants. Furthermore, the assessment strategy determines when participants earn reward points, when they are given penalty points, and when they are signified that they repeat the same mistakes, even after periodic training and reinforcement of the same knowledge and skills being assessed [24].

3.2.4 Participants

The participants characteristic refers to the attributes associated with the attendees of a CR, which can be:

- learners or trainees using a project in the context of an education and training program or a certification process,
- researchers and scientists who perform research and development,
- cybersecurity experts working in the public or private sector and evaluating cyber security technologies, tools and measures set up in the CR for evaluation of their effectiveness.

Participant attributes include:

- Their background and experience in cyber security, and the level of the participant (i.e., beginner, intermediate, advanced or professional) according his/her knowledge and skills in cyber security.
- Their needs and expectations.
- Their profession (e.g., military, police, students, government officials, cybersecurity professionals working in public and private agencies, researchers) [20].
- Their cognitive, social and cultural background.
- Their ability to assimilate new knowledge and skills [25].

3.2.5 Infrastructure

A CR may be implemented on an infrastructure using several networks with different topologies, computers and other devices [20]. The CR infrastructure can be based on:

- Equipment of the physical layer (hardware & software), which constitutes the physical infrastructure on which the CR is developed. Infrastructure consists of physical computing devices of all kinds (workstations, servers, mobile devices, etc.), network devices (e.g., routers, switches, firewalls), operating systems (e.g., Linux, Windows, Mac OS) database management systems, etc. Some CRs rely solely on physical infrastructure, but this is usually an expensive solution, which does not scale well when the number of the participants changes.
- Cloud computing technologies, especially the Infrastructure as a Service (IaaS) type, as it facilitates the construction of CRs, reduces the costs, and eases the CR's scalability.
- Virtualization technologies which allow the creation of virtual machines and networks "hiding" the complexity of the physical layer operation.
- Isolation technologies of the CR from other systems, to provide the possibility of forming a fully configurable and integrated environment not causing damage to external systems.

3.2.6 Policies and mechanisms

The policies and mechanisms characteristic is based on the features of the didactics characteristic (e.g., Environment) and determines the manner the CR project operates. For example, the CR's assessment strategy may require the red team members to collect proofs that they have solved the CR's challenges. Such proofs may be specific files (e.g., log files), screenshots and evidence of the sequence of actions followed.

CR policies may include rules that prohibit specific tools, techniques, and activities, such as attacking the workspace and the platform (e.g., the assessment system). In addition, the mechanisms of a CR may foresee the recording of the participants' actions, with particular emphasis on critical actions (e.g., actions causing changes to the score) [25].

3.3 Weaknesses

As stated in Sect. 2, there are several notable studies on CRs, though they seem to focus more on particular principles and characteristics of CRs, while overlooking others. More importantly, current studies do not diminish the requirement for economically feasible CR solutions, which was stressed out by cyber security experts during the interviews conducted

in the context of the current study as the costs of developing and organizing CRs and new scenarios are high. The conducted CR domain analysis also revealed several weaknesses, which are presented in the remainder of this section.

3.3.1 High preparation costs

The preparation phase of a CR requires a lot of resources, money and specialized personnel, as well as a long period of time that can last several months [6,26]. The CR must be a safe, legal and isolated environment from external networks and the internet, in order not to be affected by external factors and threats [27]. However, during the preparation phase many products (especially the commercial ones) require online licensing and activation processes to work. For this reason, the CR must be created from scratch, including the installation of applications and tools, the creation of network services, the provision of controlled internet access, and the creation of network data traffic [28]. Usually, the CR must mimic real systems (e.g., networks of ministries) and include computing and networking devices of all forms, as well as mobile devices and virtual users who will perform the activities of real users to create realistic data traffic during its operation [28].

3.3.2 High testing requirements

The dry run of a CR under preparation requires the involvement of specialized personnel who will go through the CR challenges in order to identify bugs, suggest improvements, and verify its reliability. The dry run should be performed long enough before the execution of the CR to provide enough time for corrections, optimizations, and adjustments [4].

3.3.3 Learning strategy neglection

Although an education and training approach must be designed on the basis of well-known learning theories, the majority of educational CRs omitted to build their teaching strategy on modern learning theories and good teaching practices. As presented in the topic map of Fig. 2, there was only a limited number of CRs which analyzed the educational perspective of CRs such as the characteristics of teaching strategy, learning objectives, participants characteristics etc. Moreover, a multidisciplinary and complex field, such as cybersecurity education, requires the formation of continuous and multi-layer learning environments. A multi-layer learning environment provides educational approaches that adapt to the needs and expectations of learners, as the layers of learning include different degrees of difficulty, which increase the complexity and challenge levels. A continuous learning environment aims at enhancing trainee readiness by

providing a) an environment that is always available for education and training, b) opportunities and motives for periodic reinforcement of trainees' knowledge and skills.

3.3.4 Fixed workspace

There are many CRs, which are useful for specific activities or types of exercises. Once learners find the solutions to the challenges and achieve the learning objectives, the CR workspace should be modified. Otherwise, it is considered obsolete as it is no longer useful [6].

3.3.5 Ineffective assessment

Assessment strategies usually award points to the learners when they solve a challenge, or they do not award points at all. Besides, assessment strategies do not take into consideration the methods and techniques the learners apply, or whether they have encountered difficulties in an early or a late stage of an exercise (e.g., in the beginning of the exercise or just before the end) [6].

3.3.6 Participants profiles

Organizers of the CR projects do not keep records of the participants' profiles, and they usually have limited knowledge about the background of the learners. For this reason, they often fail to create exercise scenarios tuned to the learners' needs, expectations, and level of expertise. As a result, in some cases learners are not challenged enough by the CR challenges, and they do not engage because they consider obsolete the activities they have to perform in the CR workspace. On the other hand, in some cases learners face difficulties to perform the activities of the CR workspace and they are discouraged.

4 The proposed cyber range design framework

In this section, the Cyber Range Design Framework is presented as a means to facilitate the development of effective CRs and to confront the identified CRs' weaknesses. The elaboration of such a framework is considered necessary, as there are very few studies on the design of CRs that holistically considered the subject (presented in the Related work section). Besides, the CR domain completely lacks methodological frameworks based on learning theories, instructional strategies, standards and models that have already been utilized in cyber security education. For this reason, CRDF is elaborated on the basis of the COFELET framework by fusing the characteristics and the weaknesses of CRs, along with the components of the COFELET game architecture and the

phases of the Exercise Life-Cycle. For the elaboration of CRDF, the design and creation methodological approach was employed [29], according to which CRDF has been produced as a result of a process of reforming and extending the COFELET game architecture and the Exercise Life-Cycle (analytically presented in Sects. 4.2 and 4.3, respectively), in order to embrace the characteristics of the CRs, and confront their weaknesses. In the remainder of this section the CRDF framework is presented along with the COFELET and Exercise Life-Cycle that formed its foundations.

4.1 Foundations

4.1.1 COFELET framework and architecture

COFELET (Fig. 3) has been chosen as one of the pillars of the presented study, as it is a multidisciplinary framework for the development of cyber security education approaches, such as serious games based learning. COFELET features the proposed approach, as it is established on the principles of modern learning theories (i.e., activity theory and constructivism), and it specifies the main elements that must be taken into consideration when developing COFELET compliant approaches, known as COFELET approaches.. In conjunction with the framework, the COFELET ontology is utilized, which analytically describes the key elements of COFELET approaches (e.g., tasks, learning objectives), and the way they must be associated in the structure of such approaches to support their learning and the instructional aspects. On the contrary with the related studies in the CR domain (presented in Sect. 2), COFELET considers the manner the key elements contribute to the achievement of the requirements and the confrontation of challenges of cyber security education [7] in terms of effectiveness, economic feasibility and appeal to a wide range of people.

COFELET foresees cyber security educational approaches which infuse the pedagogical elements with the users' actions, as it analyzes the COFELET approaches under the gaming, the learning and the instructional perspectives. The gaming perspective interprets the actions performed in a COFELET approach (e.g., the learners' actions) towards the fulfillment of the goals; the learning perspective explicitly relates the learners' actions with accomplishments of learning objectives and the possession of KSAs; and the instructional perspective considers the actions a COFELET approach performs to assess the learners' actions and to scaffold their efforts. User actions are represented by the Task elements (represented in the upper part of Fig. 3 by unnamed circles). The tasks are organized into Scenario Execution Flows (SEFs) elements, which determine the sequence of tasks users have to perform to achieve their goals. The condition elements are the prerequisites that must occur to make

the tasks performable, whereas the goal elements are the aims the task sequences achieve.

The learning objectives (LOs), the knowledge, skills, and abilities (KSAs), the hints and the teaching contents are the pedagogical elements, i.e., the elements related with the learning and the instructional perspectives of the COFELET approaches. LOs are short statements which describe the KSAs aimed to be fostered in learners, whereas hints are the suggestions provided to the learners to help them achieve the approach's goals, and teaching contents include text, figures, and videos explicitly related with the KSAs and the learners' actions. A session is set up according to a COFELET scenario, which contains the appropriate information such as the scenario's goals, the conditions, the entities (i.e., distinct concepts that lie in the context of a COFELET approach). The COFELET framework envisages the development of scenarios of varying difficulty and challenging level according to the learner's profile, the target LOs, the learning strategy, and the educational environment where the approach is conducted (i.e., educational context). During a session, a COFELET approach monitors, assesses, and supports the learners' efforts. At the end of a session, the learner's profile and learning history are updated and in the subsequent sessions, new scenarios are selected for the learner with respect to the learner's profile and history, the target LOs, and the educational environment.

The aforementioned elements are analytically described in the COFELET ontology presented in [8,9]. The tasks, the conditions and the goals are the primary elements of the COFELET ontology, which along with the pedagogical elements provide the basis for the definition of the SEFs and the scenarios. The manner the COFELET ontology elements are incorporated and organized in the structure of a COFELET approach (i.e., a COFELET game), along with the major components of such an approach, is depicted in the COFELET game life-cycle (Fig. 4), and it is analytically presented in the [8].

The COFELET game life-cycle is specifically proposed as a blueprint for the development of COFELET games and it consists of two phases: the Run-Time and the Build-Time phases. The Build-Time phase involves the creation of the COFELET ontology elements including the SEFs and the scenarios, whereas the Run-Time phase specifies the functions that have to be performed during a game session. The Run-Time phase also exhibits the typical architecture of a COFELET compliant game (COFELET game architecture), which includes the main components of a COFELET game, the components' interconnections, and the functions these components are accountable to perform. Specifically, the COFELET game architecture illustrated in the Run-Time phase of the COFELET game life-cycle includes:

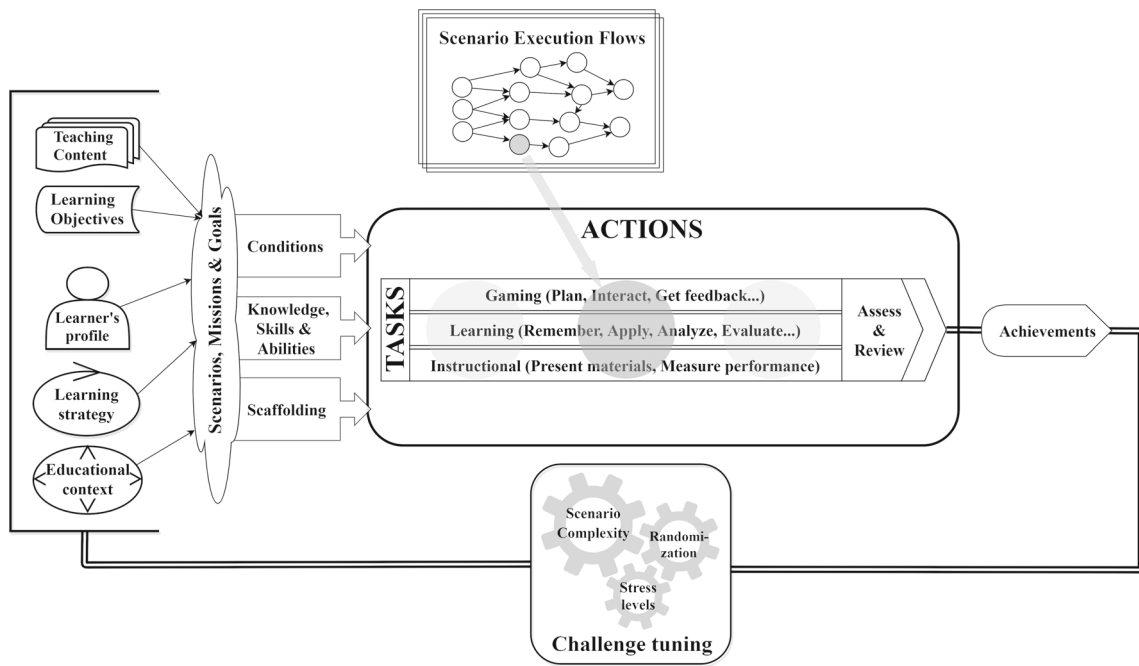
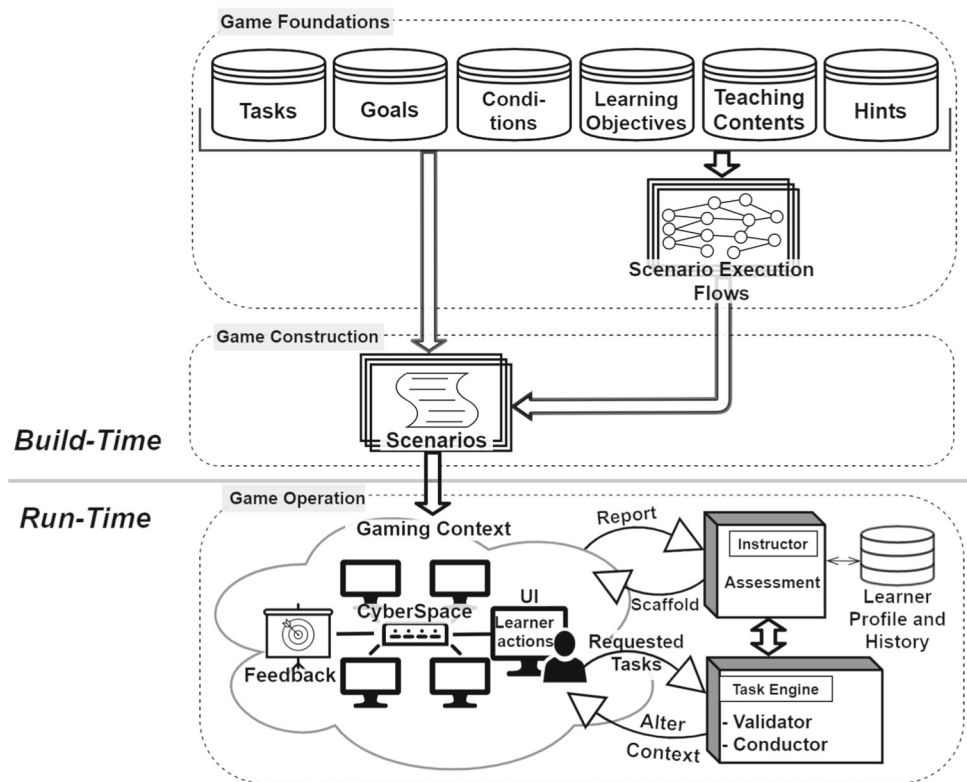


Fig. 3 The COFELET framework [7]

Fig. 4 The COFELET game life-cycle [8]



- Gaming Context, which contains the learner’s user interfaces (UI), the cyberspace in which learners perform their tasks and the feedback provided according to the performed tasks.
- Task Engine, which validates and performs the learner’s tasks in the cyberspace by affecting the entities’ state (e.g., payload creation, starting a remote connection to a host) and changing conditions (e.g., learner acquired the information related to a vulnerable service running on a target host such as service name and version).
- Instructor, which monitors and assesses the learner’s tasks and scaffolds learners’ efforts.
- Learner Profile and History, which stores the learner’s details and the learning history.

Furthermore, COFELET foresees cyber security educational approaches that adopt well-known models and strategies generally used in threat analysis and modeling approaches such as the MITRE’s Common Attack Pattern Enumeration and Classification (i.e., the CAPEC classification of attack patterns), the MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (i.e., the ATT&CK knowledge base) and the Lockheed Martin’s Cyber Kill Chain (CKC). For example, the COFELET scenarios’ attacks is proposed to be defined in analogy to the CAPEC’s attack patterns or the TTPs of the ATT&CK knowledge base, whereas in a scenario presented in the [30] the CKC model was used as a guide for the consideration of the attack strategy and its steps.

4.1.2 Exercise life-cycle

Researchers in [4] defined the Exercise life-cycle based on the Plan-Do-Check-Adjust (PDCA) cycle consisting of the following phases which can be repeated:

1. Preparation: the goals are set, the scenario is formed, the infrastructure is created, etc. Preparation is the most demanding phase of the Exercise Life-Cycle, as it requires the consuming of significant time and resources, and the involvement of specialized personnel.
2. Dry run: the CR is checked for errors; adjustments are made, and its integrity is checked.
3. Execution: involves the execution of the CR according to the specified scenario.
4. Evaluation: participants’ efforts and progress are evaluated. The evaluation results are reported during the CR execution phase, and after the CR execution phase accompanied by comments and rewards. The evaluation phase may include the conducting of research and the organizing evaluation workshops.

Finally, the evaluation results are interpreted by the exercise organizers and instructors. According to the evaluation results, the phases of the Exercise Life-Cycle can be repeated to improve the effectiveness of the exercise.

4.2 CR architecture

A CR is used for organizing and operating CR Projects. The proposed CR Architecture (Fig. 5) depicts the main parts of a CR (i.e., CR Infrastructure, CR Workspace, and CR Platform), the manner these parts are organized, and the ingredient parts they contain. In our approach, we consider that a CR builds upon the CR Infrastructure part and includes a set of dynamic elements (elements whose properties change at run time according to the characteristics of the intended CR Project), which form the CR Workspace part and a set of static elements, which form the CR Platform part.

CR Architecture adopts the design considerations of the COFELET framework and the COFELET game architecture (described in the Sect. 4.1), but it also considers the CRs key characteristics presented in Sect. 3. Thus, CR Architecture embraces the main components of the COFELET game architecture, but it additionally extends them by involving additional parts, functions and features necessary for the development of CRDF approaches compliant with the COFELET framework. More specifically:

- CR Workspace is defined in analogy to the Cyberspace of the COFELET game architecture, but the CR Workspace features the formation of a realistic cyberspace consisting of real devices and virtual machines.
- The Coach and the Registry components of CR Platform encompass the functions of the Instructor and Learner Profile and History components of the COFELET game architecture respectively.
- The User Interfaces, Feedback and Reports components of CR Platform adopt the functionality of the UI and feedback of the COFELET game architecture, but they also extend it by including more capabilities (e.g., integration of user interfaces for the instructors, inclusion of reports)
- As in the COFELET game architecture, CR Architecture involves a repository of scenarios and scenarios’ elements.
- CR Architecture does not require a Task Engine which validates and performs the learners’ tasks performed in CR Workspace, as it is a realistic environment and not an emulated one.
- CR Architecture requires a component (i.e., the Tracker component) which monitors the state of the components of CR Workspace. In the COFELET game architecture such a component is not required, as the cyberspace and its entities are interconnected and managed by the Task Engine.

- CR Architecture requires components (such as the Automations component) that will automate procedures and functions (e.g., the setup of devices and VMs) in order to mitigate the set up and the running demands, and to enhance the realism aspect of the CRDF approach (e.g., generation of network traffic). In the COFELET game architecture the cyberspace is accountable for the setup and operation of the emulated hosts and devices according to the entities and the conditions specified in the game's scenario.

The remainder of this section presents the constituent parts of the CR Architecture.

4.2.1 CR projects

CR Projects offer educational and training programs in cyber security, assessment procedures for certification of knowledge and skills, tests and experiments for research purposes, as well as cyber security competitions and exercises. Specifically, an education and training program is a sequence of educational activities designed and organized with the aim of achieving predefined learning objectives or the completion of a specific set of educational tasks within a specified period [31]. Cybersecurity certification requires the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance [32]. Cybersecurity exercise is a planned event during which an organisation simulates cyber-attacks or information security incidents or other types of disruptions in order to test the organisation's cyber capabilities, from being able to detect a security incident to the ability to respond appropriately and minimise any related impact [10].

4.2.2 CR platform

In general, a platform consists of a set of technologies used as the foundation on which applications, processes and services can be developed [33]. CR Platform contains the permanent and stable components of a CR, which provide automation processes such as the creation of virtual machines and the virtualized network (routers, firewall, servers, etc.), network traffic simulation, installation of software packages (browsers, e-mail management applications, etc.), mass creation of network user accounts, monitoring of the CR Workspace state, and visualization of information for the instructors and the participants [28].

The CR Platform's composition is modular, so that common functions are utilized by various components and scalability possibilities for upgrades and extensions are offered. The CR Platform's components must comply with standards to ensure their interoperability and reuse. These components

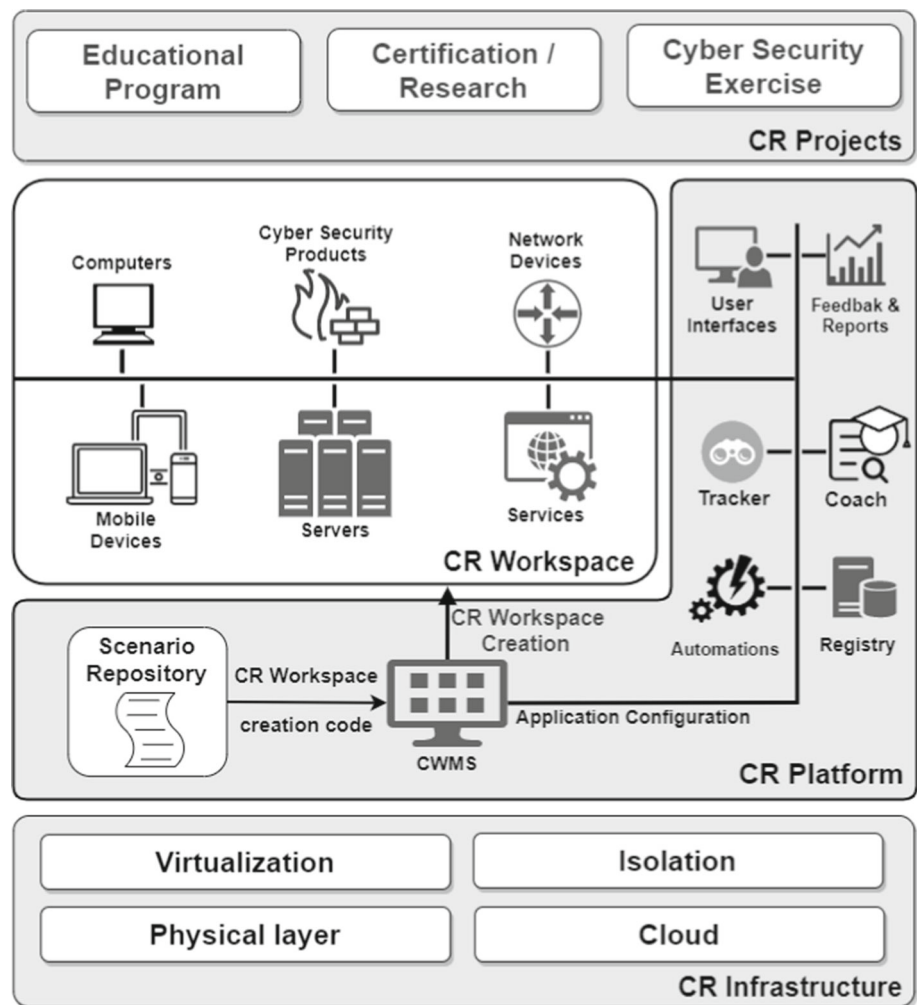
are isolated from CR Workspace and the communications with the elements of CR Workspace are restricted and moderated. The CR Platform's components can be developed from scratch, or they can be implemented by leveraging, customizing, and configuring open-source solutions, such as network traffic generators and data visualization applications.

4.2.2.1 CWMS CWMS automatically creates the appropriate CR Workspace by interpreting the scenario of a particular CR Project. It implements a critical subsystem of CR Platform, providing a central web-based interface for instructors, researchers, and organizers. CWMS contains the organizer or instructor interface, which offers the controls for the development and the management of CR Workspace (e.g., scenario selection from the repository, modification of the CR Workspace). Instructors will use the CWMS interface to search into the scenario repository and select the appropriate scenario based on the learning objectives and the learning strategy, the learners' characteristics, the features and the constraints of the environment where a specific CR Project is conducted (e.g., in a workshop of a cyber security training organization or at home with participants connecting remotely to CR Workspace). CWMS uses the Infrastructure as a Code (IaaS) approach to interpret the code contained in the scenarios and to automatically generate the required CR Workspace. In addition, through the CWMS interface instructors will be able to review the generated CR Workspace, modify it by adding and removing elements, configure it by adjusting the appropriate settings, review the records of participants (profiles, learning history, targeted knowledge and skills etc.), define the participants in a CR Project and divide them into groups. CWMS will communicate with the rest of components of CR Platform and based on the scenario and the instructors' settings, it will orchestrate the operation of the rest CR Platform components (e.g., which actions will be recorded, how many points the coach component will reward on a successfully unleashed cyber-attack, etc.).

4.2.2.2 Tracker Tracker monitors the status of the CR Workspace's components, the network traffic, and the participants' actions. Specifically, it retrieves information from CR Workspace and tracks the actions performed by the participants of a CR Project. Such information regard:

- the state of services, processes, and applications,
- the existence of files, and their creation/deletion and modification,
- rules of firewalls and Intrusion Detection Systems (IDS),
- network data traffic,
- creation/deletion of users, user rights and sessions,
- updates of software and device drivers.

Fig. 5 The proposed CR architecture



The Tracker's information is collected from multiple sources (e.g., service availability checks, network traffic analysis, commands entered into a terminal by the participants) [13], and it is analyzed and correlated to lead to secure deductions on the participants' actions. The development of the Tracker components can be based on well-known tools already used in CRs such as Tcpcdump, Wireshark, Nagios, Snort, Netflow and OSSIM [13,19].

4.2.2.3 Coach Coach plays the role of a virtual instructor, which evaluates the participants' efforts by comparing the participants' actions with the scenario's solutions. When it is necessary (e.g., Tracker does not detect any action towards the right direction for a certain period), Coach scaffolds the learners' efforts by presenting a set of hints and the teaching contents that are associated with the learning objectives of a CR Project. When a CR Workspace is created, Coach receives the scenario's details from CWMS regarding the sequences of actions the learners must perform to reach the goals of the CR Project (scenario's solutions), and the assessment rubric which contains the evaluation strategy. In terms

of COFELET ontology, a scenario's solution is a sequence of SEFs learners have to apply including sequences of Tasks, along with the conditions that have to occur. During a CR Project implementation, Coach:

- receives information from the Tracker's components regarding the participants' actions, their response times to the scenario's challenges and the number of actions they perform,
- compares the learners' actions with scenario's solutions,
- checks whether the learners have managed to perform the appropriate actions within the time frame provided by the assessment rubric,
- displays hints and related teaching contents, and alerts the instructor, when learners achieve a goal, it utilizes the assessment rubric to assess and grade the learners' performance based on:
 - the time it took the learners to perform the necessary actions,
 - the total time it took the learners to achieve the goal,

- the number of actions the learners performed,
 - the number hints provided to the learners,
 - details from the learners' learning history regarding the number of times they participated in a CR Project that had the same or a similar scenario, the number of times they exercised the associated knowledge and skills.
- communicates the assessment results to the sibling components of CR Platform (i.e., the Registry, and Feedback and Reports components).

4.2.2.4 Registry Registry manages the CR Platform database, which maintains the records of the participants (i.e., learners, trainees, companies and organizations) according to data received from Tracker and Coach (e.g., grades, number of hints provided to the learner/trainee, etc.). Moreover, it provides the required learning history details to Coach such as the scores awarded in previous CR Projects in the same or similar scenario.

Specifically, the registry of companies or organizations includes:

- the expertise and type of services they provide (e.g., cyber security audits, digital forensics, protection against Denial-of-Service cyber-attacks),
- a list of employees,
- the time required to respond to service requests,
- the length of time it can provide services,
- indicative costs per service,

The records of learners or trainees include:

- the background (age, profession, etc.),
- the learning history in CR Projects:
 - scenarios participated,
 - the achieved goals,
 - the exercised knowledge and skills,
 - scores,
 - the times learners/trainees required to achieve the scenarios' goals,
 - the number of actions performed to achieve the scenarios' goals,
 - the amount of assistance needed in Educational CRs
- the knowledge and skills they possess,
- the target knowledge and skills,
- the teams participated in (e.g., blue, red, white, etc.)
- the roles assumed in CR Projects (e.g., penetration tester, forensics investigator, malware analyst, etc.),
- certifications,
- readiness level according to:

- the number of CR projects participated in,
- the frequency of updating and reinforcing their knowledge and skills.

4.2.2.5 Feedback and reports The amount of data that needs to be examined and evaluated by cyber security experts during an attack is very large [34]. For this reason, the visualization of the exercise's data is a key utility in upgrading the effectiveness of management of cyber security exercises [35]. A data visualization component, such as the Feedback and Reports component, can help cyber security experts understand quickly and at an abstract level the course of a cyber-attack, and possibly to identify it in time and prevent its recurrence [36]. Moreover, the Feedback and Reports component needs to get and process data at real time to help organizers and participants to make decisions as the cyber-attacks progress [26].

In the CR Platform, the Feedback and Reports component receives data from the Tracker, and the Registry components and transforms it in the appropriate format (e.g., charts, tables, statistics) for better appreciation and evaluation of results. It utilizes data visualization components to present:

- representations of the evolution of cyber-attacks occurring in a CR Project (unleashed or about to be unleashed),
- the score changes of teams participated in a CR Project,
- the display of the team score,
- the elements of CR Workspace (e.g., representation of the network topology).

For the development of the Feedback and Reports component, the Security Information and Event Management (SIEM) tools can be utilized, such as the open SIEM AlienVault OSSIM [34]. Additionally, the Integrated Scoring and Awareness Tool (ISA) can be utilized, developed by CybExer Technologies, which was awarded the NCIA Defense Innovation prize in the data visualization category [37]. The ISA tool monitors the teams' scores and provides a visual representation of the evolution of cyber-attacks that take place in the context of a CR project [35].

4.2.2.6 Automations The Automations component includes mechanisms which automate functions of CR Workspace to generate network traffic, virtual user accounts that perform virtual actions (e.g., use of the CR Workspace services), and automated cyber-attacks. Network traffic generation enhances the fidelity and realism [38] of CR Platform. Network traffic generators inject legitimate and malicious traffic into the network to simulate the realistic operational network traffic [23]. Malicious traffic is different in nature from the traffic of typical users, although it may involve actions similar to those performed by system administrators such as detecting available ports on the network, creating and changing

passwords in user accounts and installing software products [28]. Network traffic generators must simulate traffic of different protocols (e.g., HTTP, SMTP, POP, FTP, ICMP), and provide facilities for the specification of the source, the destination, the duration and the quantity of the produced traffic [39]. Some of the network traffic that can be utilized in the automations component are the Tcpreplay, which is used to replay recorded traffic from routers, firewalls and intrusion prevention systems or IPS; the IXIA BreakingPoint which can work both at the software and hardware level, while it has the ability to generate network traffic in the form of packets based on specific protocols; the TRex is an open source software developed by CISCO that can generate network traffic installed in a virtual machine (VM) [23,38].

4.2.2.7 User interfaces User Interfaces (UIs) for the instructors and the participants are used to provide various capabilities including web-based interaction with CR Platform and CR Workspace.

Instructor UI provides controls for the management and the monitoring of CR Projects and for the collaboration with the participants, organizers, and other instructors. Specifically, instructor interfaces will provide the following capabilities:

- assignment of graded access levels for participants and instructors and granting of access from all types of devices (e.g., computers, tablets and mobiles),
- connection and configuration of the CR Platform's components,
- connection and configuration of the CR Workspace's components,
- access to the details of the participants stored in Registry,
- monitoring of the participants' activities,
- presentation of the CR's results in real time and sorting of results by participant, by team, by role, by organization or company,
- review of the CR Workspace status (e.g., infected files, non-functional services),
- communication with the participants (e.g., through a chat system), and provision of help, guidance and feedback (e.g., brief instructions, animations, teaching content etc.),
- communication with colleagues and organizers,
- elaboration of reports and completion of assessment forms regarding the participants' performance and the efficiency of a CR Project,
- printout of certificates.

Participant UI provides the following options:

- overview of the CR Project status through a subsystem (dashboard), which will present information such as the

scoreboard, the CR Project goals and the percentage of goal achievement, teaching contents etc.

- access to the computing and the network devices of CR Workspace,
- access to the participant profile and learning history stored in the Registry,
- presentation of results in real time and sorting of results by participant and by team,
- printout of certificates,
- communication with teammates and instructors, through a subsystem which will provide facilities for reading and sending messages, for requesting help, etc.

4.2.2.8 Scenario repository The Scenario Repository component contains the CR's scenarios and their constituent elements. A scenario is created in accordance with COFELET scenarios consisting of the CR Project's goals, the scenario's entities (i.e., the CR Workspace's components) and the scenario's conditions. The scenarios' elements include:

- Virtual machines and network devices, utilized as templates during the CR Workspace creation,
- IaaS scripts for CR Workspace creation and deployment,
- COFELET ontology elements (e.g., SEFs, entities),
- Configuration files of the CR Platform components (e.g., the assessment rubric files of Coach, setup files of Tracker defining sources of information, traffic to be monitored etc.). Scenarios are categorized according to their features such as the target learning objectives, the characteristics of the participants, the features of the environment where a CR Project will be executed, and the learning strategy to be employed. The scenario's elements are grouped according to their features such as the type of element (e.g., computers, devices, scripts), the scenarios in which they were utilized, the software and firmware included, etc. The Scenario Repository component also provides a search facility for the scenarios and the scenarios' elements based on the previously mentioned features of scenarios and scenarios' elements.

4.2.3 CR workspace

CR Workspace is the cyberspace in which participants perform their activities and it consists of multiple components including virtual or physical computers, mobile devices (e.g., laptops, tablets, mobile phones), network devices (e.g., routers), servers, services (e.g., world wide web services such as DNS, webmail, and websites), integrated technologies (e.g., smart grids, cyber-physical systems), wireless sensor networks, etc [12,40]. In some CRs (e.g., CRs of test type), CR Workspace additionally contains the cyber security products to be evaluated such as tools (e.g., antiviruses, firewalls,

Intrusion Detection Systems), technologies (e.g., advanced security mechanisms such as authentication and access control, real-time intrusion detection systems), and policies and procedures related to cyber security.

The CR Workspace's components are dynamic, as they vary according to the type and the characteristics of a particular CR Project. CR Workspace is created in an automated manner by CWMS, based on the scenario selected by the instructor, and acquired from Scenario Repository. The CR Workspace's components communicate and cooperate with the CR Platform's components during the CR Project's execution, and especially with the Tracker component which continually scans the state of the components and the Automations which generate traffic and execute the virtual users' activities.

4.2.4 CR infrastructure

In general, with the term infrastructure we usually consider the physical and/or virtual resources of hardware (servers, computers, network equipment, storage media, etc.) and software (services and applications for network management, monitoring, recording, remote connection, network traffic generation, etc.) used for the development of a platform. The CR Infrastructure components are Physical layer, Cloud, Virtualization and Isolation.

4.2.4.1 Physical Level Physical Layer determines the fidelity of the CR, and it consists of networks, servers and storage devices. CRs can rely exclusively on Physical Layer, which is a high-fidelity approach, but expensive and inflexible due to the lack of scalability and reuse. To address these limitations, CR Infrastructure usually utilizes virtualization and cloud computing technologies.

4.2.4.2 Virtualization With the adoption of virtualization technologies, economically viable CRs can be created, which can simulate efficiently any digital infrastructure. Such technologies utilize the hypervisor software to ensure that virtual machines (VMs) do not interfere with each other and that they have access to the physical resources they require to operate. The hypervisors can be available as commercial software (e.g., VMware, Parallels, Microsoft Hyper-V, IBM z/VM), or open-source software (e.g., KVM, Virtual Box, QEMU). Virtualization can also be based on the technology of containers, which have been very popular in recent years. Containers improve the portability of applications and fast and reliable execution because they integrate in a software component the code of an application along with the application's libraries and dependencies. Multiple containers can run on a single machine, as they share the machine's operating system. Docker is the most popular choice for container-based virtualization.

Virtualization includes the advantages of dynamically assigning computing resources to VMs; restoration of systems that are saved as snapshots; rearrangement and reconfiguration of network infrastructures; easy addition, cloning, modification and deletion of elements. The main disadvantage of virtualization is the downgrading of the infrastructure's fidelity when the realistic simulation of an organization's infrastructure is a fundamental requirement.

4.2.4.3 Cloud The utilization of cloud computing technologies helps at the exploitation of the physical computing resources in the most efficient way, as the hypervisor has the ability to manage all available resources, allowing their optimal exploitation and distribution.

CR deployment can be based on a public cloud, a private cloud or a hybrid approach that combines both approaches. In public cloud CR infrastructures, the infrastructure is managed exclusively by the cloud service provider (e.g., Amazon, Microsoft, Google). In such cases, users access services without having to engage with the infrastructure management. Key limitations of this approach are the lack of control over the data moving to and from a CR Project, the lack of flexibility in developing and configuring scenarios, and the obliged compliance with technological limitations set by the cloud provider.

In private cloud CR infrastructures, the infrastructure is created and managed by the CR organizers, who assume the cost of installation, maintenance, and operation. A key advantage of this approach is the full control of both the deployed applications, the data and the information circulating in the cloud infrastructure. The private cloud computing is preferable in cases where privacy and confidentiality are required (e.g., when CRs are elaborated for the government or the military), since public cloud computing is an open system that can become more vulnerable to cyber-attacks.

A hybrid cloud CR infrastructure is the optimal solution for the proposed approach as it has the advantages of both the public and private cloud infrastructures, providing control over the security of the CR data (private) and having infrastructure scalability (public).

4.2.4.4 Isolation Isolation foresees the separation of CR Projects from the operating system, virtual machines, and containers running on the same hardware. CR Projects must be isolated from external networks and systems to be secure and fully controlled. Virtualization employed with VMs, and hypervisors offers high levels of isolation, and they are stable. On the contrary, virtualization employed with containers has lower levels of isolation, as containers have a direct dependency on the operating system sharing many elements that can interfere with each other.

4.3 CR life-cycle

The CR Life-Cycle (Fig. 6) is a proposed roadmap for presenting the high-level activities of developing CRDF compliant CRs. The CR Life-Cycle adopts the phases of the Exercise Life-Cycle of [4], but it also proposes three additional phases which present the manner CRDF approaches can be designed and deployed under the viewpoint of producing feasible economical solutions composed of reusable elements. The proposed CR Life-Cycle is based on the ADDIE development model [41], the Plan-Do-Check-Adjust cycle, and the COFELET game life-cycle (presented in Sect. 4.1 and illustrated in Fig. 4). To support reusability, it involves the COFELET ontology elements [8], which facilitate the design and creation of the CR Workspace components.

More specifically, the proposed CR Life-Cycle (Fig. 6) consists of the following phases:

1. *Analysis* involves the exploration of the participants' and environment's characteristics, the determination of the learning objectives and the learning strategy which will help participants to fulfill these objectives. The participants' characteristics include information on the participants' details, capabilities, background, as well as the learning history stored in the Registry component. The environment characteristics (i.e., the educational context of the COFELET framework) include the features and the constraints of the environment, where a CR Project will take place.
2. *Design* is defined in analogy to the Build time phase of the COFELET game life-cycle (Fig. 4). The Design phase determines the scenario and the required SEFs as solutions to the scenario's challenges. The SEFs and the scenarios are created by the combination of the COFELET ontology primary elements (i.e., the tasks, the conditions, and the goals), the pedagogical elements (e.g., LOs, KSAs, hints, teaching materials) which are stored in the repository of elements. Scenarios include the following parts:
 - A *Cyberspace* which is a blueprint for the development of CR Workspace, as it defines the entities (e.g., computers, devices, services etc.) describing the CR Workspace components it must contain (e.g., virtual machines and devices, services), and the conditions it must involve (e.g., vulnerabilities that must be infused in the CR Workspace components).
 - *Steps* which define the stages participants must follow to accomplish the CR Project's mission and fulfill the CR Project's objectives. Each step includes sub-goals, a set of conditions (i.e., pre-conditions and post-conditions) and a set of pedagogical elements analytically described in [8]. According to the COFELET framework, the Steps' goals match the SEFs' goals, while the SEFs define the sequence of tasks the participants must perform to achieve the Steps' goals. The step's pedagogical elements associated with the learning perspective include the learning objectives defined in a formal and detailed manner, along with the related pedagogical elements associated with the instructional perspective for the provision of help, guidance, and feedback to the participants (e.g., instructors' tips, scenario's hints, and teaching contents).
 - *Attributes* which describe the details of the scenario including name, description, difficulty level and complexity.
3. *Configuration* based on the defined cyberspace and entities, the components of CR Workspace are created along with the corresponding IaaS scripts. The Configuration phase features the design consideration of the COFELET framework [8], according to which COFELET compliant approaches consist of a set of configurable and reusable elements for the facilitation of development of such approaches. Under this perspective, the configuration phase involves the utilization of predefined components (e.g., virtual machines of computing and network devices deployed from templates, infrastructure as a code scripts) acquired from the scenario repository, as well as the creation of new reusable components. Finally, the CR Project components are set, and the suitable configurations are arranged for their proper operation and cooperation with the CR Workspace components.
4. *Deployment* components prepared in the Configuration phase are combined, the network is created along with the network devices, and CR Workspace is established. The operations of the CR Workspace components are tuned, as well as their cooperation with the CR Platform components. The corresponding IaaS scripts are finalized to automate the creation of CR Workspace. Cyber security products are deployed, and their installation and configuration are documented and stored in the scenario repository.
5. *Dry run* the effectiveness and the integrity of the deployed CR Workspace are evaluated and verified by cyber security experts.
6. *Execution* the deployed CR Workspace is used by real participants (e.g., learners, trainees, researchers, and experts) in real settings and for the purposes of a specific CR Project. The effectiveness of the deployed CR Workspace is evaluated based on the feedback received by the instructors and the participants', and on the analysis of the participants' performance.

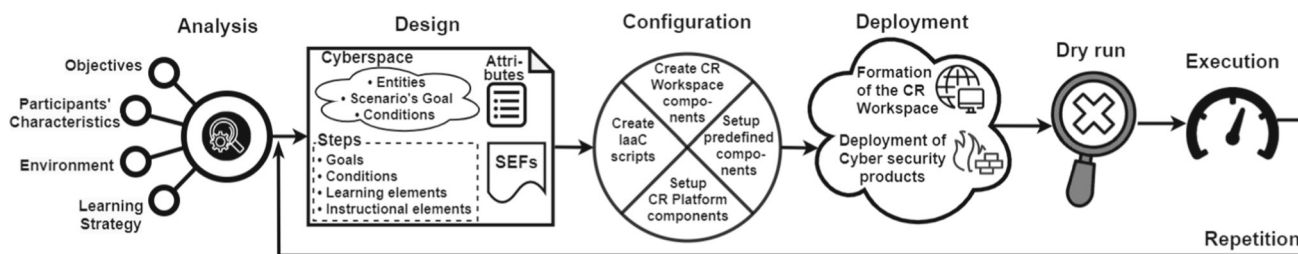


Fig. 6 The proposed CR life-cycle

The results of the evaluations (produced during the Dry Run and Execution phases) provoke reflections on the scenario's effectiveness, and possibly modifications on the deployed CR Workspace, and reconfiguration of the CR Platform components. According to the COFELET framework, the complexity and the stress levels of the scenario can be tuned by the re-design of the scenario's cyberspace and steps. For example, the complexity of a scenario can be increased by the expansion of the CR Workspace's entities and conditions, and the increase of the number of steps participants must consider advancing in a CR Project. The stress levels can be increased by making the assessment rubric stricter over time. Therefore the phases 2 to 6 are executed repeatedly.

5 Preliminary evaluation

CRDF foresees the development of efficient new CRs confronting the weaknesses of already analyzed CRs. Although the CRDF framework is yet to be tested through the development and assessment of CRDF approaches, a preliminary appreciation of its impact can be deduced based on the innovative features and design guidelines such approaches are specified to embrace, and the weaknesses they seem able to address. Table 1 contrasts the identified weaknesses (presented in Sect. 3.3) against the features and the design guidelines of the proposed approaches. The column Addressed specifies whether the weakness is expected to be mitigated (symbol '✓'), or not mitigated (symbol 'X'), whereas the column Design guidelines explains the rationale of the Addressed specification.

6 Discussion

This section discusses the features and the expected outcomes of the proposed approach.

6.1 Strengthening of cyber security education and training

The proposed framework is expected to strengthen the impact of cyber security education and training programs by pro-

viding continuous and adaptive training. Also, it contributes to the increase of cyber security expert's workforce, and the fostering of the necessary knowledge and skills to the existing cyber security personnel as it gradually helps them face new challenges in the field of cyber security. Besides, CRDF facilitates the creation of Certification CRs aiming at strengthening the readiness of professionals in cyber security and especially the readiness of professionals working in critical infrastructures in the public and in the private sectors. Cyber security professionals should periodically participate in cyber security exercises to certify and reinforce knowledge and skills and test their level of readiness while receiving assessment certificates. In addition, the proposed approach supports the creation of high-validity and high-fidelity Test CRs, which simulate real networks and systems at a high degree of realism, and they include cybersecurity products. The conducted tests contribute to the research and development in cyber security through the trial use and evaluation of new technologies, tools and protection measures; and through the communication of results to the involved parties, the discussion of results and the drawing of conclusions.

Additionally, the proposed approach provides opportunities for the formation of appropriate teaching approaches aiming at raising the awareness of the public in cyber security and especially the awareness of the personnel working in the public and private sectors. Finally, by utilizing gamification and simulation techniques, new CR Projects will offer teaching approaches that stimulate the interest of new generations, as they will help young learners overcome the difficulties of comprehending basic cyber security concepts and of acquiring basic skills. In such a way, more younger individuals will pursue a career in cyber security.

6.2 Conformance with standards

CRDF conforms with well-known standards of cyber security and cyber security education, as it is elaborated on the foundation of the COFELET framework. Through its conformity with the COFELET framework, CRDF envisages the utilization of genuine technologies (e.g., simulations, gamification techniques), innovative learning strategies (e.g., activity theory [8]), and well-known cyber security standards such as

Table 1 Addressed weaknesses against proposed design guidelines

Weaknesses	Addressed	Design guidelines
Preparation demands		
High budget	✓	CRDF foresees economically feasible CRs, as they consist of predefined components (e.g., template VMs, IaaS scripts, reusable scenario elements), and they include automation mechanisms for the creation and the execution of CR projects. The proposed CR Life-cycle presents the manner that economically feasible CR approaches can be designed and deployed
Resources	X	CRDF compliant CRs utilize virtualization, isolation and cloud technologies, which facilitate their development. However, this guideline is not a new feature, as it is already applied in the majority of modern CRs
Specialized personnel	X	CRDF-compliant CRs require the involvement of specialized personnel. This guideline is not a new feature, as it is already applied in all modern CRs
Workspace requirements	✓	CR Workspace's creation is prescribed by the scenarios stored in the Scenario Repository component. CR Workspace's creation includes on demand installation of applications, deployment of services, provision of controlled internet access, and generation of network data traffic
Testing requirements	X	CRDF-compliant CRs demand high testing requirements. This guideline is not a new feature, as it is already applied in the majority of modern CRs
Fixed workspace	✓	The CR Workspace's components are dynamic, as they are created according to the scenarios, and they vary according to the type and the characteristics of the CRs, and the characteristics of the participants and their learning history (stored in the participants' records in Registry)
Modern learning theories	✓	CRDF is based on the COFELET framework, which embraces a rich repertoire of modern learning theories and strategies [7], particularly focusing on the learning and instructional aspects of CRs
Layered learning	✓	CRDF envisages CRs as multi-layer learning environments through (1) provision of a wide range of scenarios, (2) scenario selection according to the participants characteristics and the envisaged learning strategy, (3) dynamic creation of educational CR Workspaces
Continuous learning	X	CRDF compliant CRs do not embrace the always available environment for cyber security training and education
Ineffective assessment	✓	CRDF foresees approaches with advanced assessment capabilities, as they continually monitor the participants' actions and evaluate their efforts. Tracker monitors the actions performed in CR Workspace, whereas Coach dynamically assesses the efforts of the participants by comparing the participants' actions with the scenario's solutions
Participants profiles	✓	The Registry component of the proposed CR Architecture, maintains analytical records of the participants, organizations and companies

the MITRE ATT&CK, the MITRE CAPEC, the Lockheed Martin's Cyber Kill Chain model, and the NIST's NICE framework, which are generally used in the threat analysis and modeling. CRDF embraces the COFELET ontology and the COFELET game architecture in order to determine the elements of the CRDF approaches, and the manner these elements are interconnected in the structure of the CRDF approaches.

6.3 Architectural design

CWMS, as a critical component of CR Workspace, facilitates the development of all types of CR Projects (education and training programs, research, and cyber security exercises) and provides CR organizers with the following capabilities:

- Creation of high-fidelity CR Workspace
 - Installation of software and services.
 - Creation of complex infrastructure consisting of different networks and topologies.
 - Configuration of the infrastructure.
 - Automated creation of virtual machines and virtual devices.
- Injection of vulnerabilities.
- Repository of scenarios for the preparation, the operation and the evaluation of CR Projects.
- Maintaining a back-end storage facility (the participants' registry) of the participants' profiles and their learning and training history.
- Dynamic assessment of participant's performance.
- Communicating and visualizing the results of CR Projects (e.g., teams' scores, degree of success of cyber-attacks, etc.).
- Provision of elevating scaffolding facility to support the learners' efforts (Educational CRs).

CRDF envisages the utilization of automation mechanisms and tools, such as the open-source programs Ansible (for server configuration), Terraform (for the creation and management of infrastructure based on code), Vagrant (for the creation and management of virtual machines).

6.4 Layered learning environment

Learners should perform activities adapted to their abilities and needs. CR Architecture includes a repository of scenarios of elevated difficulty: low, medium level, and advanced. Low difficulty scenarios will require learners to identify, comprehend and remember concepts, structures, facts, and practices. Medium-level scenarios will require trainees to perform simple missions by exercising the knowledge and skills of the low-difficulty scenarios. Advanced scenarios

will require learners to demonstrate advanced knowledge and skills to solve realistic challenges and authentic problems.

6.5 Online learning environment

New CR Projects will include web-accessible and always available activities for the practicing and the training of cybersecurity professionals and for the enhancement of their mission readiness. It is widely accepted that the basic knowledge and skills of cybersecurity professionals tend to decay if they are not exercised regularly in the context of their daily work duties [42]. For this reason, CR Platform maintains in the participants' registry, the learning history indicating the knowledge and skills exercised by the participants along with the scenario they were exercised, the awarded grades, and the timestamp of the scenario execution. Based on the participants' learning history, the CRDF approaches will provide motives and opportunities for learners to periodically reinforce their knowledge and skills by engaging in genuine scenarios and challenges.

6.6 Adaptive learning environment

CRDF foresees the development of CRs which provide an interactive environment in which learners can practice advanced cyber security techniques until they achieve the learning objectives of acquiring the target knowledge and skills. When the learning objectives are achieved, the environment dynamically adapts to keep high the learners' interest and motivation in two ways: (a) it provides to learners the opportunity to practice the acquired knowledge and skills in new manners in order to increase the mastery of knowledge and skills and to enhance the readiness of the trainees, (b) it fosters new knowledge and skills by presenting new scenarios with different types of exercises [43]. CWMS provides the ability to dynamically configure and adjust CR Workspace [6].

6.7 Scenario-based learning

CRDF adopts the scenario-based learning approach. The scenarios contain the appropriate information for the creation and the execution of the CR Projects. A scenario contains code for the automated creation of CR Workspace (e.g., creation of virtual machines and web devices, installation of software, injection of vulnerabilities), and the necessary configuration settings such as the CR Project goals, the assessment strategy, the hints presented to the learners that need help, teaching content, the actions learners must perform to solve the CR Project challenges, etc.

6.8 Dynamic assessment

During the execution of a CR Project, the learners' efforts are monitored and recorded in the participants' registry. At the same time, the learners' efforts are assessed by comparing the actions performed by the participant with the actions foreseen in the scenario of the CR project. According to the performance of the learners and the assessment strategy, which are detailed in the particular CR Project's scenario, feedback and help will be provided to the learner, and information will be reported to the instructors. The evaluation strategy has the form of a rubric that awards points to learners based on their performance in the CR Project execution (the time it took the learner to possess the learning objectives of CR Project, the number of hints the learner required, the number of actions the learner performed, etc.), and the details stored in the learning history kept in the participants' registry (e.g., how many times the participant performed the same or a similar scenario which involved similar learning objectives, knowledge and skills, etc.).

6.9 Multi-role user support

CR Platform provides to users a distinct interface, depending on their role and the group they belong to, as follows:

- Learners or trainees (especially military personnel, law enforcement officials, personnel working in critical infrastructures in the public and private sector) have the opportunity to apply and update their theoretical and practical knowledge in a suitable CR Workspace [44]. Learners, in addition to participating in courses and exercises, have the opportunity to participate in specially designed test and certification CRs to obtain recognized certificates in the field of cyber security (e.g., CEH, CISM, CISSP, CCSP, CASP, GSEC, SSCP, CISA, GCIH) [45]. These CRs help to identify talents and create “talent pools” from which members can be drawn to form national cybersecurity frontlines.
- Trainers utilize suitable CR Workspaces for the education and training of learners, for the evaluation of the learners' knowledge and skills they have acquired through the activities offered. The trainers also contribute to the development of the learning objectives, the scenarios, and the teaching content of CR Projects.
- Academic community (scientists, researchers) contribute to the development of new CR Project scenarios or the exploitation of the existing ones [46]. Members of the academic community also contribute to the creation of a digital library with:
 - specially designed educational material,

- tools for carrying out offensive and defensive ethical hacking actions,
- prefabricated virtual environments [47],
- serious games specially designed for education and training in CR Projects.

In addition, the contribution of the academic community may include the organization of competitions and events, with topics related to cyber security [47], but also conducting research to understand the ways the CRs are used by the instructors [48].

- Professionals and specialized personnel working in various organizations and fields such as cyber security, information technology (IT), law enforcement, forensic investigation and cyber security incident response [44]. Skilled professionals may contribute to the testing and the evaluation of products, tools, and settings related to the cyber security of the organizations' actual network infrastructure.

6.10 Collaboration between public and private sector

Aiming at the cooperation of public and private sectors, at attracting investments and at strengthening the actions of the involved organizations, various CR Projects can act as a collaboration point for companies and organizations. Companies involved in cyber security will be able to be engaged in CR Projects as participants (e.g., for training or certifying the company's employees) or as co-organizers (e.g., for research, development and evaluation of new products and services). CR Platform keeps the profiles of the participating companies and organizations (including information on their expertise and the services they can provide), and the employees (e.g., targeted knowledge and skills, roles they assume in CRs, learning history, certified knowledge, readiness level, accreditations) in the Registry component.

7 Conclusions

As cyber security is a top priority concern for governments, corporations, and individuals, the strengthening of cyber security education and training is of major importance. In this study, the CR domain, particularly focusing on CRs utilized in formal education settings and in the organizations of cyber security exercises and competitions, was explored. To this end, the CRs' key characteristics and weaknesses were identified and categorized. By reflecting on the performed exploration and by utilizing the COFELET framework, a framework particularly elaborated for the development of cyber security educational approaches, the Cyber Range Design Framework was proposed. CRDF is expected to guide

the development of effective CRs which will involve the appropriate features for the exploitation of the CRs' qualities and the conformance of the analyzed CRs' weaknesses. An initial appreciation of the CRDF impact showed that CRDF approaches involve several advanced features, which can ensure the effectiveness and the cost-efficiency of the CRs developed. Such features are the application of a scenario-based approach, the use of automation mechanisms and the reuse of elements, the adaptation to the participants' capabilities, the inclusion of advanced assessment capabilities, and the adoption of gamification techniques. CRDF is expected to form the basis for the development of various purpose CRs aiming at delivering effective cyber security education and training; assessing the participants' knowledge and skills in the cyber security (e.g., certification); and evaluating the effectiveness of cyber security products (i.e., technologies, tools, protection measures). Moreover, the CRDF approaches can be utilized to train citizens in cyber security awareness and promote positive cyber security culture among young learners.

Acknowledgements This work has been supported in part by a grant offered by the Hellenic Ministry of Digital Governance to the Research Center of Athens University of Economics and Business (2022-24).

Funding Open access funding provided by HEAL-Link Greece. This study has been partially funded by the Hellenic Ministry of Digital Governance.

Data availability All data generated or analyzed during this study are included in this published article.

Declarations

Conflict of interest None of the authors have received a speaker honorarium from any company. All authors declare that none of them has any conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Malekos Smith, Z., Lostri, E.: The hidden costs of cybercrime (2020). <https://www.mcafee.com/enterprise/en-us/assets/reports/rphidden-costs-of-cybercrime.pdf>. Accessed 20 Oct 2022
2. Morgan, S.: Cybercrime to cost the world \$10.5 trillion annually by 2025 (2020). <https://cybersecurityventures.com/cybercrime-damagecosts-10-trillion-by-2025/>. Accessed 20 Oct 2022
3. International Information System Security Certification Consortium (ISC). A resilient cybersecurity profession charts the path forward (2021). <https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>. Accessed 21 Oct 2022
4. Vykopal, J., et al.: Lessons learned from complex hands-on defence exercises in a cyber range. In: 2017 IEEE Frontiers in Education Conference (FIE). IEEE, Indianapolis, IN (2017). <https://doi.org/10.1109/fie.2017.8190713>
5. National Institute of Standards and Technology (NIST): The cyber range—a guide (2020). https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NISTNICE%29%20%28Draft%29%20-%20062420_1315.pdf. Accessed 20 Oct 2022
6. Yamin, M.M., Katt, B.: Modeling and executing cyber security exercise scenarios in cyber ranges. *Comput. Secur.* **116**, 102635 (2022). <https://doi.org/10.1016/j.cose.2022.102635>
7. Katsantonis, N.M., et al.: Conceptual framework for developing cyber security serious games. In: 2019 IEEE Global Engineering Education Conference (EDUCON). IEEE, Dubai, United Arab Emirates (2019). <https://doi.org/10.1109/EDUCON.2019.8725061>
8. Katsantonis, M.N., Mavridis, I., Gritzalis, D.: Design and evaluation of COFLET-based approaches for cyber security learning and training. *Comput. Secur.* **105**, 102263 (2021). <https://doi.org/10.1016/j.cose.2021.102263>
9. Katsantonis, M., Mavridis, I.: Ontology-based modelling for cyber security e-learning and training. In: International Conference on Web-Based Learning. Springer, pp. 15–27 (2019)
10. European Cyber Security Organisation: Understanding cyber ranges: from hype to reality. Technical report (2020)
11. Russo, E., Costa, G., Armando, A.: Building next generation cyber ranges with CRACK. *Comput. Secur.* **95**, 101837 (2020). <https://doi.org/10.1016/j.cose.2020.101837>
12. Ukwandu, E., et al.: A review of cyber-ranges and test-beds: current and future trends. *Sensors (Basel)* **20**(24), 7148 (2020). <https://doi.org/10.3390/s20247148>
13. Yamin, M.M., Katt, B., Gkioulos, V.: Cyber ranges and security testbeds: scenarios, functions, tools and architecture. *Comput. Secur.* **88**, 101636 (2020). <https://doi.org/10.1016/j.cose.2019.101636>. (ISSN: 0167-4048)
14. Pepper, S., Moore, G.: Topic maps. In: Encyclopedia of Library and Information, vol. 1, pp. 5247–5259 (2010)
15. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). ISO/IEC 13250: Topic Maps, 2nd Edn (2002). <http://xml.coverpages.org/TM-iso13250-2nd-ed-v2.pdf>. Accessed 22 Jan 2023
16. Rebecchi, F., et al.: A digital twin for the 5G era: the SPIDER cyber range (2022). <https://doi.org/10.5281/zenodo.6347532>
17. Razvan, B., et al.: Integrated framework for hands-on cybersecurity training: CyTrONE. *Comput. Secur.* **78**, 43–59 (2018). <https://doi.org/10.1016/j.cose.2018.06.001>. (ISSN: 0167-4048)
18. Davis, J., Magrath, S.: A survey of cyber ranges and testbeds executive. In: Defence Technical Information Center, Fort Belvoir (2013)
19. Chouliaras, N., et al.: Cyber ranges and testbeds for education, training, and research. *Appl. Sci.* **11**(4), 1809 (2021). <https://doi.org/10.3390/app11041809>

20. Priyadarshini, I.: Features and architecture of the modern cyber range: a qualitative analysis and survey. Ph.D. thesis, University of Delaware, Newark, DE, USA (2018)
21. Nicodeme, B.: Federated cyber range challenges. MA thesis, Université Libre de Bruxelles, Belgium (2019)
22. Cambridge Dictionary. Federation. <https://dictionary.cambridge.org/dictionary/english/federation>. Accessed 20 Oct 2022
23. Cyber-MAR. D2.1: State of the art cyber range technologies analysis (2020). https://www.cyber-mar.eu/wp-content/uploads/2020/06/Cyber-MAR_D2.1_State-of-the-art-Cyber-range-technologies-analysis_v1.0.pdf. Accessed 20 Oct 2022
24. Nagarajan, A., et al.: Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, Bangkok (2012). <https://doi.org/10.1109/CYBER.2012.6392562>
25. Katsantonis, M., Fouliras, P., Mavridis, I.: Conceptual analysis of cyber security education based on live competitions. In: 2017 IEEE Global Engineering Education Conference (EDUCON). IEEE, Athens, Greece (2017). <https://doi.org/10.1109/EDUCON.2017.7942934>
26. Oslejsek, R., et al.: Evaluation of cyber defense exercises using visual analytics process. In: 2018 IEEE Frontiers in Education Conference (FIE). IEEE, San Jose, CA, USA (2018). <https://doi.org/10.1109/fie.2018.8659299>
27. Urias, V.E., et al.: Cyber range infrastructure limitations and needs of tomorrow: a position paper. In: 2018 International Carnahan Conference on Security Technology (ICCST). IEEE, Montreal, QC (2018). <https://doi.org/10.1109/ccst.2018.8585460>
28. Braje, T.M.: Advanced tools for cyber ranges. Technical report, MIT Lincoln Laboratory Lexington, United States (2016)
29. Oates, B.J.: Researching Information Systems and Computing. SAGE Publications Ltd, Thousand Oaks (2006)
30. Katsantonis, M., Mavridis, I.: Evaluation of HackLearn COFELET game user experience for cybersecurity education. *Int. J. Serious Games* **8**(3), 3–24 (2021). <https://doi.org/10.17083/ijsg.v8i3.437>
31. UNESCO Institute for Statistics: International standard classification of education: ISCED 2011. In: Comparative Social Research, vol. 30 (2011)
32. ENISA: EU cybersecurity certification framework. <https://www.enisa.europa.eu/topics/standards/certification>. Accessed 20 Oct 2022
33. Technopedia: What does platform mean? <https://www.techopedia.com/definition/3411/platform-computing>. Accessed 20 Oct 2022
34. Chaskos, E.C.: Cyber-security training: a comparative analysis of cyberranges and emerging trends. MA thesis, National and Kapodistrian University of Athens, Athens (2019)
35. Foresight. D2.1 State of the Art Scenario Report (I) (2020). <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5de52f16b&appId=PPGMS>. Accessed 20 Oct 2022
36. Disney, A.: Graph visualization use cases: cyber security (2017). <https://cambridge-intelligence.com/use-cases-graph-visualization-cybersecurity>. Accessed 20 Oct 2022
37. US-Africa Cybersecurity Group (USAFACG): CR14 open cyber range: a resource to trial cyber security tools (2018). <https://usafacg.com/2018/05/15/>. Accessed 22 Oct 2022
38. Javali, C., Revadigar, G.: Network web traffic generator for cyber range exercises. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, Osnabrueck, Germany (2019). <https://doi.org/10.1109/lcn44214.2019.8990880>
39. Ministry of Communications and Multimedia Malaysia (MCOMM): Cyber range framework. https://www.cybersecurity.my/data/content_files/26/2249.pdf. Accessed 20 Oct 2022
40. Pavlova, E.: Implementation of federated cyber ranges in bulgarian universities: challenges, requirements, and opportunities. *Inf. Secur. Int. J.* **50**(2), 149–159 (2021)
41. Peterson, C.: Bringing ADDIE to life: instructional design at its best. *J. Educ. Multimed. Hypermedia* **12**(3), 227–241 (2003)
42. Allen, P.D., Straub, K.A.: Using games to enrich continuous cyber training. In: Johns Hopkins APL Technical Digest, vol. 33, no. 2 (2015)
43. Jones, R.M., et al.: Modeling and integrating cognitive agents within the emerging cyber domain. In: Proceedings of the Inter-service/Industry Training, Simulation, and Education Conference (IITSEC), vol. 20. Citeseer (2015)
44. Turčanik, M.: A cyber range for Armed Forces Education. *Inf. Secur. Int. J.* **46**(3), 304–310 (2020). <https://doi.org/10.11610/isij.4622>
45. Cyber security competence for Research and Innovation: Feasibility study “cybersecurity skills certifications (2020). <https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf>. Accessed 20 Oct 2022
46. Costa, G., Russo, E., Armando, A.: Automating the generation of cyber range virtual scenarios with VSDL. In: arXiv preprint [arXiv:2001.06681](https://arxiv.org/abs/2001.06681) (2020). <https://doi.org/10.48550/arXiv.2001.06681>
47. Petrone, J.: CR14 open cyber range: a resource to trial cyber security tools (2020). <https://e-estonia.com/c14-a-resource-to-trial-cybersecurity-tools>. Accessed 20 Oct 2022
48. Beauchamp, C.L.: Exploring cyber ranges in cybersecurity education. Ph.D. thesis, Virginia Tech (2022)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.