IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 July 2025, accepted 11 November 2025, date of publication 27 November 2025, date of current version 5 December 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3638168

SURVEY

How Accessible Is Cybersecurity Training? A Survey on the Accessibility, Capabilities, and Technology Stack of Cyber Ranges

CHRISTOPH STEININGER[1,2], **LAURA GÖTZ**[1,2], **AND MATTHIAS SCHOPP**[1]
[1]Research Institute CODE, University of the Bundeswehr Munich, 85579 Neubiberg, Germany
[2]Department of Computer Science, University of the Bundeswehr Munich, 85579 Neubiberg, Germany
Corresponding author: Christoph Steininger (christoph.steininger@unibw.de)

ABSTRACT With the escalating frequency and sophistication of cyberattacks on companies and government agencies, the demand for hands-on cybersecurity training has never been more critical. Such training requires a dedicated platform and infrastructure. In this context, Cyber Ranges have emerged as platforms to address these needs. This article systematically evaluates the current state of cybersecurity training in Cyber Ranges, with a focus on the technology stack, training features, and automation capabilities. Various dimensions are used to assess accessibility, such as access to the platform, training content, supervised training, the deployment model, or the ease of onboarding. Mapping specific Cyber Range features to these categories, we developed the Cyber Range feature ontology, which can be used to evaluate Cyber Ranges according to existing best practices, technical trends and lessons learned from current research. By combining a systematic literature review with the results of a subsequent survey, this study closes existing knowledge gaps on current Cyber Ranges and provides actionable insights for researchers and practitioners. Thereby, we also developed a web-based filtering tool that is hosted on a website to make the results even more accessible to the public. This comprehensive analysis provides insights into the current state of cybersecurity training via Cyber Ranges, facilitating an understanding of the challenges and opportunities in this rapidly evolving field. The results reveal which technologies are currently employed in Cyber Ranges, but also which groups can be trained on which topics. Furthermore, key trends and emerging themes in the field are identified.

INDEX TERMS Accessibility, automation features, cyber range, cyber range features, cyber range training, information security, literature review, questionnaire, security training, survey, technology stack.

I. INTRODUCTION

Cybersecurity has become an imperative facet of modern business and governance, given the pervasive and persistent nature of cyber threats. The threat of cyberattacks looms over organisations of all sizes and across industries. The consequences of a successful cyber intrusion can be devastating, ranging from financial losses and reputational damage to the compromise of sensitive data.

According to recent statistics, there has been a significant surge in the number and severity of cyber incidents across industries. The 2023 Boardroom Cybersecurity Report expects the global cybercrime costs to reach 10.5 trillion USD annually by 2025, up from 3 trillion USD in 2015 [1]. IBM meanwhile reports that in 2023 the global average cost of a data breach was 4.45 million USD - a 15% increase over 3 years [2]. The German Federal Office for Information Security, however, counts cyberattacks on several European state institutions, industry, critical infrastructure providers as well as governmental institutions in its management report 2023 [3]. According to IBM, cyberattacks have affected businesses in finance, healthcare, manufacturing, education, service industry and the public sector, among others, showcasing the diverse range of targets [4]. Also, small businesses, often overlooked in cybersecurity discussions, have increasingly become victims of attacks [5]. This emphasises the need

The associate editor coordinating the review of this manuscript and approving it for publication was Joao Bernardo Ferreira Sequeiros.

© 2025 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

for inclusive and effective cybersecurity training across organisations.

The sophistication and frequency of these attacks underscore the critical need for skilled cybersecurity professionals capable of defending against evolving threats. As organisations strive to fortify their digital defences, cybersecurity training has emerged as a cornerstone for preparing personnel to navigate the complex and dynamic cyber threat landscape. Thus, the accessibility of cybersecurity training becomes a critical factor in ensuring that professionals, regardless of their background or expertise, can effectively acquire and train skills. The training and preparedness of cybersecurity professionals are vital for organisations of all kinds, irrespective of their size, industry, or geographical location.

Cyber Ranges (CRs) provide a platform that allows hands-on training in a realistic network environment. It is also possible to adopt these training environments to mimic or depict an organisation's real-world productive network. Complex attacks and training scenarios can be simulated, but the level reaches from single person training to team training, and trainees can perform diverse educational hands-on activities according to their role. Moreover, CRs facilitate hands-on learning experiences, allowing participants to interact with different tools, platforms, and security protocols. The controlled and isolated nature of CRs ensures a safe space for learning, fostering the development of practical skills and experience. Hence, CRs provide a perfect platform to enable cybersecurity training for all kinds of organisations with varying needs [6].

Our survey aims to explore how accessible CRs are for diverse target groups and which needs they can address. As the needs among institutions of all sizes and different fields of operation vary, several different needs have to be addressed, ranging from the used technology stack to supervised training. Therefore, the following research questions are stated:

- What does the current Cyber Range (CR) landscape look like, and what features characterise these platforms?
- What trends in the CR landscape can be identified regarding the accessibility of such platforms and trainings?

Previous research in this field has either investigated the technologies and tools used overall without making concrete statements about their adoption, such as Yamin et al. [7], or – when comparing specific CR platforms – provided only limited and just partial information on the technologies and tools actually used, e.g., [8], [9], [10], [11], [12], [13]. Our research aims to provide a comprehensive overview of CR capabilities and characteristics to support organisations in identifying suitable cybersecurity training and to assess the current state and development of CR-based training. Information on the platforms and tools used in CRs is essential to make concrete statements about specific technology adoption, training contents, and thus, the state-of-the-art in CRs.

Current trends, however, have to be identified to anticipate upcoming developments that will impact the accessibility of CR platforms and their training offerings in the near future. In this context, the term ''accessible'' encompasses a multifaceted evaluation of various aspects related to CR platforms, which serve as pivotal environments for hands-on cybersecurity training:

- **Deployment Model:** Accessibility starts with the mode in which a CR is run. CRs may be accessible either in the cloud or on-premise. Also, hybrid approaches might be possible. Understanding the implications of these access modes is crucial for evaluating the adaptability of cybersecurity training to an organisation's needs.
- **Product Access:** Some CR products are only available for a dedicated target group. This is especially the case for CRs with a focus on military, critical infrastructures or government. Access in this case can also mean certain security requirements that have to be met, like isolation from the internet or other tenants, as well as data protection regulations.
- **Platform Access:** The means by which users access CRs significantly influence their experience and should ideally resemble the real-world procedures of an organisation. Different access methods offer varying levels of user-friendliness and security. Also, the degree of availability of the platform itself is relevant in this context.
- **Training Content:** The diversity of training content is another crucial aspect of accessibility. Examining whether CRs offer predefined scenarios, customisable modules, or the ability to create entirely new training content provides insights into the flexibility and adaptability of the training platform, which is also a varying need among organisations of different sizes and government agencies.
- **Supervision and Support for Training Design and Execution:** The level of supervision during cybersecurity training is a critical consideration. Assessing whether training is self-directed or supervised provides insights into the support, guidance and mentorship available for learners, which might be a necessity for entities that want to practice cybersecurity but do not want to run the exercises on their own. Whereas bigger companies and institutions might want to craft scenarios exactly tailored to their situation themselves, organisations with less resources or knowledge might prefer predefined trainings.
- **Includable Platforms, Systems and Software:** CRs differ in terms of the systems they can depict. This comprises the inclusion of certain software but also seamless connection, e.g., of hardware or operational technology (OT). The possibility to make certain systems or software accessible in a CR is therefore a need that has to be considered.

- **Training Evaluation and Learning Outcomes:** Assessing how CRs evaluate training sessions and measure learning outcomes is also an integral need, whereby the preferred method might vary among organisations. This dimension addresses the tools and methodologies employed for assessing participants' skills and knowledge acquisition.
- **Ease of Onboarding - Tool and Platform Adoption:** The ease with which individuals can familiarise themselves with the tools, platforms, and management software used in CRs directly influences the accessibility of training. For organisations that do not want to administrate the trainings themselves, the usability of the platform for the trainees is essential, while organisations that want to run their own on-site CR may have more wide-ranging needs. Analysing the simplicity or complexity of the setup process provides valuable insights into the feasibility of implementing such training solutions. Investigating the prevalence of widely adopted tools and platforms, as well as the existence of developer communities and support, sheds light on the learning curve associated with running and creating such environments.

By understanding these dimensions, organisations can make informed decisions for cybersecurity training, contributing to a more secure digital landscape. This survey aims to provide a comprehensive understanding of the current state of CRs, their accessibility, and their role in addressing the pressing need for effective cybersecurity training among diverse organisations' needs in the face of escalating cyber threats. With this, we contribute to foster cybersecurity education and competence.

The remainder of the article is organised as follows: In Section II, the target groups and purpose of cybersecurity training are elaborated to identify the use cases for cybersecurity and therefore the relevant capabilities of CRs. Section III presents the related work. Section IV describes our research methodology and compares it with previous research. Section V outlines the results of the survey. In Section VI, these are discussed and current trends in the field are elaborated. Section VII concludes this article with a summary.

II. USE CASES AND NEEDS FOR CYBERSECURITY TRAINING

This section first describes the target sectors, the training audience and the purpose of cybersecurity training. Based on this, use cases are defined, from which the questions and categories to be answered by this survey are derived.

Päijänen et al. [14] identify the target sectors for cybersecurity training to be companies, law enforcement, government, students and researchers, as well as military. Knüpfer et al. [6] do not specify the private sector in more detail but also name NGOs and further divide the academic sector in schools and universities.

According to Knüpfer et al. [6], the purpose of cybersecurity training is awareness, skill, communication, leadership, or collaboration training. Päijänen et al. [14] define the purpose more in relation to the training object. They name security education through competence building and assessment, cybersecurity certification, development of cyber capabilities and resilience, cross-domain organisational trainings, as well as national or international cybersecurity competitions or exercises as purpose for cybersecurity training.

As noted by Knüpfer et al. [6], the proficiency level for cybersecurity training can range from beginner to expert. Moreover, Päijänen et al. [14] found that the roles of users participating in cybersecurity training are highly diverse. According to the roles named by their survey participants, user roles participating in CR training were director (business, communication, etc.), developer, researcher, security professional, educator, sysadmin, network admin, student, job applicants, employee, and domain specialist. Thus, the participants' roles are not only limited to technically oriented user roles but also comprise non-technical ones. This shows the broad spectrum cybersecurity training addresses.

The use cases for CR training thereby vary, depending on the type and size of an organisation and its resources for such training. Therefore, several needs have to be addressed in this survey.

To support government agencies, universities, research centres or industry representatives who have identified a use case for a CR, the European Cyber Security Organisation (ECSO) crafted a checklist for CR features [15]. The ECSO is an organisation of the European Union (EU) created to implement Europe's public-private partnership in cybersecurity [16]. It is a European cross-sectoral and independent membership organisation for cybersecurity that gathers and represents European public and private cybersecurity stakeholders. The features in the ECSO checklist extend or refine the CR checklist published by the National Institute of Standards and Technology (NIST) [17] outlining key features and potential considerations of end users/groups when evaluating CR platforms. However, the ECSO does not provide a comprehensive overview of the CR market, as there is a clear focus on European CRs and only 22 CRs are named. Furthermore, most of these do not provide all the information asked in the checklist.

Therefore, we decided to use the ECSO checklist as a base and to extend and adopt it to get a list of all the accessibility features that might be relevant when selecting a CR for cybersecurity training. In the following, the categories of the ECSO checklist [15] are mapped to the accessibility categories from Section I and refined or extended to get a list of questions that have to be addressed in order to derive all the features that describe current CRs.

A. DEPLOYMENT MODEL

Which provisioning model a company prefers will vary depending on the resources available in terms of time,

personnel and hardware for operating a CR and also on the general decision as to whether a company wants to operate its own CR or only "book" CR capacities dynamically when needed. The ECSO checklist [15] addresses questions regarding the deployment model in three different categories: *Location of the Cyber Range*, *Virtualisation Platform*, and *Hardware Requirements*. Three general questions can be deducted that have to be answered by a CR product:

- Q1: What is the general deployment model of the CR product?
- Q2: On which virtualisation platform is the CR run?
- Q3: What are the hardware requirements?

B. PRODUCT ACCESS

The accessibility of a CR for different types of organisations – as well as whether specific security or legal requirements can be met – is undeniable essential when it comes to choosing a CR platform. There are CRs which are dedicated to a certain target audience, like the providers of critical infrastructures. Also, law enforcement, military, governmental institutions and even some companies have special needs regarding security, isolation or data protection regulations. The ECSO checklist addresses these questions partly in the categories *Internet Access* and *Providers* [15]. However, these categories were extended and refined to fully incorporate such special needs:

- Q4: Is the CR only meant/accessible for a certain target audience?
- Q5: Can the CR be run disconnected from the Internet or isolated?
- Q6: Can the Internet connection in a training scenario be configured for single training environments or even specific systems?
- Q7: To which data protection regulations (e.g., the EU's General Data Protection Regulation (GDPR) [18]) and security certifications (e.g., ISO/IEC 27001 [19]) does the CR align?
- Q8: How is the maintenance model and are Service Level Agreements (SLAs) and Non-Disclosure Agreements (NDAs) possible?

C. PLATFORM ACCESS

Platform access refers to both when the platform can be used by trainees and how they are able to connect to the training sessions. Depending on the CR, training might not be available 24/7 and the complexity of how to access a training varies. Furthermore, certain access modes – e.g., VPN, Web browser, etc. – might be preferred by an organisation either because of easy use or because it is similar to an organisation's real-life workflow. Such questions are addressed in the categories *Reliability* and *Scalability + Elasticity*, as well as partly by the categories *Assessment* and *Scenarios & Workflows* of the ECSO checklist [15]. Considering this, we incorporate the need to know about the specific ways in which trainees can access the training environments and deduct the following questions:

- Q9: How available is the CR platform?
- Q10: Are there any restrictions/licence models in terms of the number of users or scenarios that can be run in parallel?
- Q11: How do trainees connect to their training environments?

D. TRAINING CONTENT

Organisations' needs regarding training content vary among sectors, staff, etc. Whereas for some, generic predefined training will meet cybersecurity training needs, others will require training scenarios tailored to specific training objectives or even scenarios that mimic their real-world environments as closely as possible. Uetz et al. [20] for example describe real-world scenarios to have a realistic net-topology, assets (e.g., operating systems (OSs) and services), and activity (realistic attack flows, benign user activity, etc.). The frequency of training will also depend on an organisation's use case and therefore determine the number of training scenarios needed. In addition, the type of training required and the roles to be trained are specific to an organisation. This also holds for the needs to acquire certain certifications. These needs are addressed by various categories in the ECSO checklist [15], namely *Use Cases supported by the Cyber Range*, *Realism of the emulation*, *Attack Simulation*, *Customisation*, *Scenarios & Workflows*, *Participants*, *Capture The Flag*, and *Testing Capabilities*. From these, we derive the following questions:

- Q12: Which type of trainings does a CR allow?
- Q13: Are there training scenarios with different training focus like, e.g., critical infrastructure, forensics, Internet of things (IoT), etc.?
- Q14: Does the CR offer training that awards industry-recognised qualifications, such as Continuing Professional Education (CPE) points?
- Q15: Which user roles can be trained?
- Q16: How many predefined training scenarios are there?
- Q17: Can training scenarios be adopted to an organisation's needs or even be built by an organisation itself?
- Q18: Is there a network traffic, user, attacker, and/or defender simulation?
- Q19: How realistic are attacks conducted in the training scenarios?
- Q20: How realistically can attack sequences be retraced?

E. SUPERVISION AND SUPPORT FOR TRAINING DESIGN AND EXECUTION

Depending on the usage model and internal organisational competencies, an organisation may prefer to conduct the training alone or with the support and supervision of the CR provider. For many organisations, supervised training might be an essential requirement. In the ECSO checklist [15], this is addressed by the category *Training & Support*. We extend

and refine this by considerations about trainings for trainers and support when either self-creating training scenarios or when requesting training from the provider

Q21: Does the CR provider conduct supervised trainings?
Q22: Is it possible to have your own staff trained as trainers?
Q23: Can custom trainings be requested, or is there support when creating these on your own?

F. INCLUDABLE PLATFORMS, SYSTEMS, AND SOFTWARE

Some CR platforms might be restricted in terms of the OSs they are able to depict. Furthermore, there can be sector specific needs, e.g., some organisations might want to include special systems like OT, proprietary tools such as a Security Information & Event Management (SIEM) or self-developed software. Regarding OT systems, also the way in which a system can be mapped to a CR (simulated vs. hardware device) can matter. This is addressed by the ECSO checklist's categories *licensed/Open Source Security Tools* and *Operational Technology + Industrial Communications*. From this, we derive the following questions:

Q24: Which Operating Systems can be depicted in the CR?
Q25: Can hardware devices be included in a training scenario?
Q26: Can proprietary software or appliances (e.g., SIEM, IPS, IDS, Firewalls) be included in a scenario?
Q27: Can trainees use/upload their own software or tools in a training environment?
Q28: Is there support for OT, and how can it be included?

G. TRAINING EVALUATION AND LEARNING OUTCOMES

The preferred method of training evaluation depends on the training type. Individual training courses, for example, can be evaluated more easily and just with the support of a learning management system (LMS), while team trainings are more complex to evaluate and may require supervision by (internal or external) trainers. Also, the preferred evaluation metric can vary from a simple scoring mechanism to qualitative assessment of the actions taken. Therefore, the ECSO checklist [15] contains several categories that address these matters: *Learning Management System Integration*, *Learning Outcomes & Standard Alignment*, *Assessment*, *Assessment for Training Scenarios*, *Ease of Use*. Considering this, we formulate the following questions:

Q29: Is there an LMS included, or does the CR support any LMS?
Q30: How can the progress of trainees be monitored?
Q31: Can the training status of users or teams be saved and replayed?
Q32: What are the models/metrics for the assessment of training outcomes?

H. EASE OF ONBOARDING, MAINTENANCE, AND CUSTOMIZATION

Organisations that aim to conduct their own trainings, create scenarios, or operate a CR need staff who can easily adopt or learn the required processes. This is especially facilitated if there is sufficient documentation and support available, or if open and widely used tools and standards are used. The ECSO checklist addresses this in the *Assets Library* category [15]. However, we extended the perspective here to also incorporate the aspects of running a CR and orchestrating training scenarios:

Q33: Is there enterprise support available?
Q34: Is there an accessible developer community/forum?
Q35: Does documentation on the CR software and the scenario orchestration processes exist?
Q36: Is there a set of predefined systems that can be included in a scenario?
Q37: Can own system templates be configured and added?
Q38: Does the training infrastructure creation process support automatisation, e.g., Infrastructure as Code (IaC)?
Q39: Which orchestration software is used to configure a training environment and is there support for open variants (e.g., Ansible, Chef, Puppet,...)?

III. RELATED WORK

During the research phase for this article, no other systematic review of CRs was found that could provide actual information about the current CR landscape, the used technologies and tools, and their cybersecurity training capabilities. Some were outdated like [8], [9], [21] whereas others had a more general perspective on the topic of CRs as a cybersecurity training environment (e.g., Yamin et al. [7]). However, most were lacking comprehensible data about the used technologies and did not consider a sufficient list of CR platforms to allow general statements about the state-of-the-art. Existing surveys ask about technical features, but provide almost no information about them, or determine technical features or information about the technology stack for only a few platforms. Specific features that provide information on how to address optimisation potential such as automation are not determined comprehensively enough, or such conclusions are not considered in detail.

Leblanc et al. [9] provided an overview of 13 cyberattack and computer network operations simulation and modelling approaches. To do so, they searched the publicly available literature. The 13 platforms, which are basically an early form of CRs, were categorised as private, academic or public research, and the authors focused specifically on artificial educational scenarios rather than realistic cyberattacks. As the survey is from 2011, it provides useful insights, but due to the significant developments in the technologies and platforms, it does not allow making comprehensible statements about the current CR landscape, state of the art regarding cybersecurity trainings, and current developments. Additionally, the sample of 13 approaches would not be suitable for such a purpose.

Davis and Magrath [8] conducted a survey on 30 unclassified CRs and related computer network operations (CNO) testbeds in 2013. The study aimed at describing the platforms'

purpose and functionality in order to allow organisations to make an informed decision when considering using or implementing a CR. Thereby, also cost-effectiveness was one of the key points. However, the authors did not only cover the supported functionalities but also provided a terminology and information about specific implementations from the sectors military, government, commercial, and academia. The article identifies hardware emulation as the most realistic approach, whereas simulation is named to provide increased flexibility and scalability. In summary, the study does also not sufficiently cover all aspects of CR platforms, like architecture, management or scenarios. It does not enable statements about the current CR landscape and state-of-the-art cybersecurity trainings, and current developments and trends cannot be deducted.

Holm et al. [21] investigated 30 ICS testbeds in 12 countries. The study had a focus on the specific exercise domain of critical infrastructures and Industrial Control Systems (ICS). The authors cover testbed characteristics like the methods to implement ICS in testbeds (virtualisation, simulation, and hardware) and categorize them according to their objectives. However, although the examined testbeds address objectives such as vulnerability analysis and tests of defensive mechanisms, the objectives themselves are not described in detail. Holm et al. [21] considered the testbeds from different angles and took 30 different testbeds into account. However, the main focus was not on CRs and thus cannot provide the relevant insights into cybersecurity training via CRs, the used technologies or tools, and trends like automation.

In a systematic literature review, Yamin et al. [7] reviewed one hundred academic articles on CRs published between 2002 and 2018. They examined the features and use cases of CRs and developed a CR taxonomy and the functional architecture of a generic CR. The study especially covers training environment-related aspects, e.g., the roles/teams involved in a cybersecurity exercise (red, blue, white, orange, purple, yellow, green, autonomous). As a result, the survey provides a classification of the capabilities and functionalities of CRs, based on the information gathered. A multitude of tools and products that are implemented in CRs for purposes like simulation, emulation, management, monitoring, and traffic generation are named. Based on these results, the authors also draw conclusions on the future development of CR environments. The survey has a broad focus, which means elements specific to certain CRs, such as training content, are not considered explicitly. Thus, no specific information on the use of technologies/tools is provided that would allow conclusions to be drawn about the consolidation of technologies and tools used in CRs or the spread of certain tools, e.g., for automation. Furthermore, there is no comprehensive representation of specific CRs and their use cases and capabilities for cybersecurity training.

Ukwandu et al. [10] surveyed academic literature published between 2015 and 2020. In their literature review, they investigated 44 CRs and testbeds. The CRs were categorised according to various properties, including the area of application (Military, Academic, Commercial, Law Enforcement, etc.), the way they are offered (Private, Public, Federated), and the teaming options that are supported. Ukwandu et al. [10] differentiate the training methods gamification, mock attack training, role-based training, and exercise and also distinguish the CR platforms based on their implementation method. Based on this information, a CR taxonomy is proposed. Regarding testbeds, also the stages that a training testbed should incorporate are presented. The authors find that CRs and testbeds have to be distinguished, as CRs include way more complexity and use cases. Also, conclusions about the future developments of CRs and testbeds are drawn. However, when directly looking into the comparison table of the 44 different CRs, it becomes obvious that for the most CRs substantial information regarding technology stack, used tools, and training possibilities is not available. Automation technologies and the training content of the CRs is not part of the survey. Therefore, the survey does not provide a full picture of the actual CR landscape and its capabilities. Conclusions regarding future developments can only be drawn to a limited extent.

In 2021, Chouliaras et al. [11] provided a systematic survey of CRs developed by educational institutions in Europe and the USA from 2011 until 2021. The literature review was followed by structured interviews with technical directors or managers of 10 selected CRs. The interview included 12 questions which targeted the components used for design, creation, implementation, and operation of a CR. Initially starting from 25 CRs, features and information available about the CRs were identified, and then the structured interviews were conducted with 10 selected CRs that provided the most information. The survey had a broad scope, but it was the first to use mixed data collection methods, including both, a literature review and structured interviews. As there are only details about 10 CRs from the area of education and research, Chouliaras et al. [11] cannot provide a comprehensive picture of the current CR landscape, their technology stack, tooling, and training use cases. However, the survey does provide concrete insights into selected current CRs.

Steiner et al. [12] researched cloud-hosted, publicly-available CRs in 2022. They classify CRs based on the five categories classroom management (i), type of labs (ii), number of labs (iii), supplementary reading materials (iv), and licence management (v). Additionally, they examined the cost per student based on various factors. Steiner et al. aimed at providing a list of ready-to-use cloud-hosted CRs, which should enable students to practice hands-on activities for cybersecurity-focused courses. The analysis is meant to be used by small to medium-sized colleges and universities that need to provide hands-on cybersecurity training to their students. The study provides a list of 15 education-oriented CRs. Besides the fact that the platforms are hosted in the cloud, there is no further information about the deployment model or the technology stack. Steiner et al. conducted the only study that does provide concrete information about

training cost per student. However, the article addresses just one specific target group and contains little information about the technology stack, tools, training content, and current state of the art in CRs.

Most recently, in 2023, Lazarov et al. [13] investigated platforms for cybersecurity teaching and learning. They introduce an interactive environment that enables easy-to-use execution and management of training scenarios. However, for this purpose, they also compared their solution to existing platforms. They analysed 35 platforms for cybersecurity education and training, including CRs, software applications, and other tools. Thereby, they focused on the available cybersecurity training that the platforms provide (e.g., network security, cryptography, and malware), the supported team types (red team, blue team, yellow team), their purpose (educational, training, or research), the target group (academic, government, military, or private), and the open source availability. Furthermore, the environment types emulation, hybrid/cyber-physical, simulation, and industrial systems were distinguished. Lazarov et al. [13] find that the majority of the platforms are not distributed as Open Source and the target group is mostly the private sector. However, they identify some platforms to focus on academia, government, and military. Regarding training content, the considered platforms provide mostly web security and red teaming scenarios. The study provides complete information on the platforms analysed in almost all cases. However, as the paper had a different focus, not as many characteristics of CRs were surveyed. Many of the platforms surveyed are Capture the Flag (CTF) platforms or pentesting labs, which are usually intended for individuals but do not provide defensive, comprehensive or customised training. Therefore, they cannot offer training tailored to the needs of a specific organisation.

The above reviews provided valuable insights into CRs, cybersecurity and the used technologies. However, none provides an actual and comprehensive overview of CRs and their use for cybersecurity training. Furthermore, detailed information about the technology stack and the used tools is missing in most cases. Consequently, it is not possible to deduct the current state of CRs and cybersecurity training and the current developments and trends.

IV. METHODOLOGY

This section outlines the methodology of this survey, starting with a systematic literature review (SLR), complemented by the development of a structured questionnaire to address significant data gaps. We then developed a CR feature ontology that enables a comprehensive description of the accessibility of CRs. Finally, we compare our approach and dataset with previous research.

A. SYSTEMATIC LITERATURE REVIEW

A SLR enables a thorough and comprehensive analysis of a broad range of academic and industry sources. In this study, it serves as the methodological basis to assess the accessibility of CRs for cybersecurity training by integrating insights from both research and practical implementations. This approach ensures both comprehensiveness and methodological soundness while advancing knowledge in this rapidly evolving domain.

The review follows the established eight-step process proposed by Okoli and Kira [22]: (1) defining purpose and objectives, (2) establishing a research protocol, (3) literature search, (4) screening for inclusion, (5) screening for exclusion, (6) systematic information extraction, (7) analysing results, and (8) writing the review.

The specific objective of this review is to identify and evaluate the current state of the accessibility of cybersecurity training in CRs. Looking at cybersecurity certifications or cybersecurity courses in general is not the scope of this article. Instead, the focus is on hands-on cybersecurity training conducted in CRs. It must be considered what training categories and capabilities CRs offer but not how individual platforms combine these into a course programme. Goals include:

- To survey available CRs for cybersecurity training.
- To identify and describe all technical features and capabilities affecting the accessibility of cybersecurity trainings on CRs.
- To cluster CRs by functionality, focus and target groups.
- To support organisations in finding suitable cybersecurity training options.
- To examine automation in CRs as it is needed for efficient operation and use.
- To comprehensively assess CR accessibility for cybersecurity training.

Between December 2023 and May 2024, the authors collaboratively conducted the SLR. Based on established guidelines, a common methodology was agreed upon, and shared resources – such as a remote bibliography, collaboration documents, and screening templates – were created. In addition to scientific sources, the authors decided to leverage available academic networks and contacts, which is good practice to extend a SLR [23]. They agreed to not only consider information in English, but also in German, as relevant information from direct contacts would possibly be available in German due to their affiliation with a German research institute.

A keyword-based search was performed using advanced queries: ''Cyber Range'' or ''Cyber-Range'' + ''platform'' or ''exer-cise'' or ''training'' or ''product'' or ''design'' or ''review'' or ''survey''. The databases IEEE Xplore, Springer Link, Wiley Online, ScienceDirect and ACM were investigated for articles published between 2014 and 2024. The process was supplemented by manual searches, reference tracking, and expert input, as recommended by Fink [24] and Briner and Denyer [23]. Key research projects in the CR domain such as ECSO [16] and CONCORDIA [25] were also included.

Given the focus on practical accessibility, not only academic literature but also information directly from commercial or Open Source CR products was considered. Such information was gathered via targeted Google searches based on platform names identified in the literature or via academic networks.

The search resulted in over 1000 scientific artcles and online results. Many were position papers, proof-of-concept implementations, testbed-specific implementations, or described related systems like CTF platforms, which typically lack coherent training scenarios. CTF platforms do not support full-fledged cybersecurity training exercises, as they mostly demand only loosely connected tasks and not coherent training scenarios [26]. As Beuran et al. [26] note, any cybersecurity training platform must support: (1) content representation, (2) environment management, and (3) training facilitation. Since we are specifically seeking fully functional CR products that can be used for cybersecurity training, we have developed the following inclusion and exclusion criteria to initially identify relevant research.

Inclusion Criteria:

1) Articles in English or German language.
2) Security exercises that present or describe a specific CR.
3) Articles regarding CR federation.
4) Articles describing or presenting one or many specific CRs.
5) Articles that used one or several CRs for validation or evaluation of results.

Exclusion Criteria:

1) Articles that mention testbeds not in the context of cybersecurity.
2) Articles that describe cybersecurity exercises that are not conducted in a CR.
3) Proof-of-concept implementations which neither are being further developed nor represent a fully-functional CR product.
4) Position papers.
5) CR architecture or concept proposals which provide no concrete implementation.

In order to include only significant and high-quality contributions, additional quality criteria were defined and used to further filter the identified research papers. Since we aim to provide insights into the accessibility of CR training based on the accessibility categories described in Section I, the questions assigned to these categories and formulated in Section II must be answerable. Also, platforms have to fulfil the CR definition stated in Section I.

Quality Criteria:

1) CRs which are not clearly available as a product (Open Source or proprietary) or which are not available via a code repository or vendor website are excluded.
2) The CR must allow hands-on cybersecurity training.
3) The CR must allow depicting real-world and complex network structures.
4) The CR must enable coherent and tailored training-scenarios.
5) Platforms that only provide CTF-style training are excluded.
6) Information regarding license and deployment model has to be available.
7) Information on whether the availability of the CR is restricted has to be available.
8) Information about how trainees can access the training environment has to be available.
9) Information about possible training types has to be available.
10) Information about training scenarios has to be available.
11) Information on whether supervised training is offered has to be available.
12) Information on which systems and software can be included into the CR has to be available.
13) Information about training evaluation and assessment possibilities have to be available.
14) Information regarding support and documentation of a CR has to be available.
15) Information about the underlying technical platform has to be available.

For Open Source and commercial CR products, the following additional criteria had to be fulfilled:

1) Information in English or German is available.
2) Contact information is available.
3) Legal requirements (e.g., Impressum on the website) are fulfilled.
4) For Open Source projects, the latest commit has to be within a time span of one year from the access date to ensure active development of the project.

Based on the defined criteria, literature screening was conducted in three stages. The keyword search yielded 1031 results from the selected scientific databases. In the first stage, articles mentioning one or more specific CR platforms were identified. In the second, information on those platforms was extracted and compiled into a consolidated set. Newly mentioned platforms were added to the set, while duplicates were noted but not included multiple times. Consequently, our research does not indicate how often a specific CR was cited. In the third stage, quality appraisal criteria were applied to exclude platforms from the set that did not meet the requirements.

In total, 73 CR platforms were identified from the literature. These were combined with CRs known from academic networks and the ECSO [16] and CONCORDIA [25] projects, resulting in a final list of 78 platforms.

During our analysis, we observed highly inconsistent data availability regarding the 39 questions identified in Section II. Several relevant features were either not mentioned in publications or could not be found via vendor websites or search engine. Therefore, we decided to create a structured questionnaire to fill the gaps and to give a bigger picture of the CR landscape.

B. QUESTIONNAIRE DESIGN

To design a suitable questionnaire, we followed established guidelines from [27], [28], and [29]. For this purpose, the 39 questions from Section II were refined into 73 more specific and elaborated questions. This ensures that all the information needed to answer the 39 questions is obtained from the study participants. In addition, the refinement ensures that the requirements for good questionnaire design are met.

Chowdhury et al. define a questionnaire as a structured and standardised tool for data collection, commonly used with a quantitative or mixed-methods approach. Its purpose is to address research questions and achieve the intended objectives, which are often aligned with respondents' preferences, attitudes, opinions, behaviours, or factual information. Such a questionnaire provides both closed and open-ended response options, allowing participants to express their views on various topics and to make evaluative judgements [27].

Following the identified guidelines, a review of the goals and objectives of the research was made. These are described in detail in Section I. For the administration of the questionnaire, we chose to use a web survey and let the informants fill it out on their own. This decision was made as the target audience consists out of computer experts all over the world. They have the needed knowhow and this ensured that the questionnaire could be accessible regardless of the time zone, location or time of day. The questionnaire was implemented in the tool SoSci survey [30] as the researchers' institution was offering the tool. The first page of the questionnaire included an introduction outlining the study's purpose, researcher details, and data protection information. The final page featured a thank-you message and contact details for further queries.

Based on Chowdhury et al. [27], specific questions were derived from and structured around the overarching questions described in Section I. Krosnick [29] emphasises that open-ended questions are appropriate when the full range of possible responses to a categorical question is unknown and when an ''other, please specify'' option is insufficient. To identify the complete set of potential answers, he recommends pre-testing with the target population using open-ended questions, compiling the responses into a comprehensive list, and then using this as a basis for closed questions if suitable. Additionally, if a numerical response is needed, it is best to ask directly for the number.

Following this conclusion and the sequence of actions by Chowdhury et al. [27], we created drafts of the questionnaire, gave them to people with expertise in our institution and only created closed questions where possible and with regard to the survey's objectives. The final questionnaire was divided into the eight blocks *A* to *H*, according to the categories in Section I.

The sequence of questions in the questionnaire is not linear; there are conditional branches. For example, some questions are shown or hidden depending on the answer given regarding the deployment model of the CR platform (on-premise or cloud). The flowchart of each block of the questionnaire as well as the specific questions and their answer options are included in the appendix in A-B. There, it is also stated how a question was designed (open, single choice with closed options, etc.). In cases where closed answer options are offered for selection, we derived these on the basis of expert interviews in combination with the experience of the research team. Sometimes a preliminary Internet search was conducted in addition.

1) BLOCK A AND Z: GENERAL QUESTIONS AND DEPLOYMENT

The first block comprised 14 questions aimed at collecting general information about the CR and its deployment model. Initially, participants were asked about their affiliation, the name, and the origin or development of the CR platform in the general questions (block *Z*). The following block *A* focused on the deployment model.

For on-premise CRs, respondents were asked which virtualisation technologies were used. Regarding the virtualisation technologies, various statistics by different companies and market researchers exist, e.g., by 6sense [31]. As common statistics often conflate hypervisors and broader architecture frameworks (e.g., VMware vSphere vs. OpenStack or Proxmox), the questionnaire specifically listed common virtualisation technologies – VMware, Hyper-V, KVM, XenServer, and VirtualBox – while allowing additional entries to cover less common solutions or alternative architectures, including cases where no virtualisation is used.

For cloud-based CRs, this block gathered data on supported cloud providers. For both deployment types, the question was posed whether container solutions were used. Containers encapsulate standard OS processes and their dependencies, representing OS-level virtualisation [32]. All containers per system are collectively managed by the kernel of the underlying OS. In contrast, as Sharma et al. [32] state, Virtual machines (VMs) which are virtualised by a hypervisor, are hardware level virtualisation. Here, each VM runs its own OS and applications on the server's resources that are managed by the hypervisor.

Additional questions targeted hardware requirements. For cloud CRs, this included network bandwidth, defined as the maximum data transfer rate. For on-premise setups, requirements regarding the use of multiple servers or cluster operation was of interest.

Availability models were also addressed, including whether the CR can be deployed on customer infrastructure, in their cloud environment, as a pre-installed product, or as a transportable version. These types of availability target CRs that are sold as a platform. Furthermore, access methods were queried, such as availability via browser-based web/cloud interfaces, VPN, or exclusively within the provider's training centre. This mainly concerns platforms that act as CR training providers.

2) BLOCK B: QUESTIONS REGARDING PRODUCT ACCESS

Block B contained nine questions focused on how the CR product can be accessed. This included whether the CR product is tailored to one or more specific target groups and whether access is restricted accordingly. To avoid confusion, both questions featured info icons with brief examples. The first question was not aimed at whether only a certain group can access the CR, but whether the content is specialised for a group. The second question, however, was aimed at finding out such restrictions.

For on-premise CRs, the questionnaire continued with the question whether Internet access is required for the CR platform itself, e.g., if the backbone services require an Internet connection, rather than the individual training environments. The goal was to find out whether the product can be operated offline. An info icon clarified this. Another question asked whether specific training environments, its network segments, or individual systems could be selectively connected to the Internet. A training environment was defined – via info icon – as the trainee-accessible network(s) during a CR training, distinct from the platform's core or backbone systems that are only accessible by the administrators. A similar question was posed for cloud-based CRs.

Further questions addressed the maintenance model, again clarified by an info icon explaining that this means update delivery (over-the-air vs. on-site), update cycles, and support. A follow-up asked about the availability of SLAs.

Another item inquired about compliance with data protection regulations and security certifications. The final question asked whether NDAs can be defined.

3) BLOCK C: QUESTIONS REGARDING PLATFORM ACCESS

Block C included five questions focused on how the CR platform can be accessed. With the first four questions, we addressed potential access restrictions, such as limited availability during office hours and licensing-related constraints. These covered user access, the number of training environments that can run in parallel, and restrictions on simultaneous scenario use. The final question asked in which ways trainees access their virtual training environments.

4) BLOCK D: QUESTIONS REGARDING TRAINING CONTENT

Block *D* included 16 questions aimed at identifying the training content offered by a CR product. First, we focused on the types of training provided, with options based on Knüpfer et al. [6]. There were brief descriptions via info icons, which included:

- *Red vs. Blue*: separate teams for attack and defence,
- *Red/Blue Mixed*: teams perform both roles simultaneously,
- *CTFs*: competitive, real-time cybersecurity challenges, often in a time-constrained, gamified setting,
- *Individual Training*: solo exercises,
- *Team Training*: group tasks focusing not only on technical aspects and skills, but also on collaboration,
- *Table-Top*: theoretical planning of cyber operations and countermeasures using speech, text, or multimedia.

If any predefined type was selected, there was a follow-up question whether the CR focuses on a specific training type. Furthermore, in this question block we also covered officially recognised training or certifications (e.g., CPEs), and what points or certificates are awarded for completing training.

Subsequently, we queried the availability and access to preconfigured scenarios. A scenario was defined (via info icon) as an individual or team task/mission within a specific training environment carried out in a CR. Further questions asked about scenario categories and the number of individual or team training scenarios available. In addition, customisation options for existing scenarios (e.g., network structure, systems, attack paths) and the question of whether customers and/or providers can apply them were examined. Beyond that, it was also queried whether customers and/or providers can design their own CR scenarios from scratch.

Additionally, we asked which user roles can participate in training, with role definitions based on Knüpfer et al. [6]. The final four questions, however, dealt with scenario dynamics, their availability and implementation:

1) Network traffic generation: whether and how network traffic is created (live or replayed) to simulate realistic conditions and generate more realistic ''noise'' in the logs, and digital artefacts.
2) User simulation: implementation of simulated normal user behaviour to increase activity and realism.
3) Defender simulation: simulation of defensive behaviour in response to attacks, but also preventive.
4) Attack simulation.

For attack simulation, we distinguished four options: (1) *Automated live attacker system* or (2) *Manually controlled live attacker system*, both of which generate highly realistic traces for the trainees. Here, the attacks are actually carried out by an attacker system in a functioning manner. In contrast, (3) *attack generators* are dedicated systems or appliances that generate traces on the trainee systems. However, the attack sequences implemented in these systems are usually not as advanced and well-designed as when executed via live attacker systems. They generate more background noise and usually more attacks in sequence. In the case of attack simulation via (4) *injects / poisoning*, artefacts are, for example, copied to the target system. This means that, unlike in real attacks, only selected artefacts and log files would be available (e.g., from an exploit execution) – not the full range of system logs and events generated during an actual attack execution.

5) BLOCK E: QUESTIONS REGARDING SUPERVISION AND SUPPORT

Block *E* consisted of four questions focused on the level of supervision and support provided for training design and execution. The first topic addressed whether the vendor offers supervised training, i.e. sessions led or supported by the

CR provider or equivalent. The second question explored whether a train-the-trainer program is available, in which the CR provider trains customer personnel to enable them to independently conduct future training on their own. The third question asked if customised training, including scenario creation and implementation, can be requested from the provider. If it was specified in the preceding block that customers can create their own scenarios, we asked whether support is offered to assist with the development of these custom scenarios and training sessions.

6) BLOCK F: QUESTIONS REGARDING INCLUDABLE PLATFORMS, SYSTEMS, AND SOFTWARE

This block comprised 12 questions focused on the platforms, systems, and software that are or can be included in the CR product. It started by asking which systems typically make up a CR training environment to identify common system types, architectures, and any prevailing approaches. The following question addressed which OSs can be virtualised within the training environments.

For both cloud and on-premise deployments, we asked whether hardware devices can be integrated into training scenarios and which interfaces are required for this. Support for OT was also addressed, as OT integration is crucial for scenarios involving critical infrastructure or industrial environments. These components often cannot be fully virtualised due to their functional or physical dependencies, especially considering cyber-physical impacts such as direct or indirect physical damage on the hardware caused by cyberattacks. If OT support was confirmed, a follow-up question asked how it is implemented.

We then asked whether proprietary software or appliances – such as SIEM, IDS, IPS, or firewalls – can be included in scenarios. Another question focused on whether trainees are allowed to upload and install their own tools or software within the training environment. This could include anything from client-side applications and server packages to full appliances, and may involve both Open Source and proprietary software. Next, we asked whether memory and disk images can be collected from systems within the training environment, either via a platform feature or manually on the systems. The final question in this block asked if trainees' client workstations (e.g., personal notebooks) can be directly connected to their respective training environments.

7) BLOCK G: QUESTIONS REGARDING TRAINING EVALUATION AND LEARNING OUTCOMES

Block *G* included four questions focused on training evaluation and learning outcomes. The first question asked whether an LMS is available. An LMS refers to a software platform designed to manage, organise, monitor, report, automate, and facilitate the delivery of educational courses, training programs, instructional materials, or professional learning initiatives [33]. We also asked whether integrating an external LMS is supported.

We then asked whether trainee or team progress can be monitored. With the last question of this block, we queried if the actions of trainees or teams can be saved and/or replayed. This can be used to visualise a trainee's effective and less-effective actions, which can be part of trainee and team evaluation after the CR training.

8) BLOCK H: QUESTIONS REGARDING ONBOARDING, MAINTENANCE, AND CUSTOMIZATION

The final block (*H*) comprised nine questions focusing on the ease of onboarding, maintenance, and customisation. The first question asked whether enterprise support is available, which means assistance when self-operating a CR. This was followed by a question on the presence of a developer community or forum that can help solve technical issues and offer peer support.

We then addressed the availability of platform documentation, essential for operation, troubleshooting, or further development – especially for the customers, but also for the CR provider. Similarly, the next question asked whether documentation is available for the scenario orchestration process, which helps understand and guide the preparation and execution of training scenarios. It can also be used as a guideline for creating new training scenarios. These benefits are internal for the platform provider, but also external for a potential customer who purchases a CR platform.

The next question focused on whether a predefined system library is available to simplify and accelerate scenario creation. The system templates in such a library already provide certain systems that no longer need to be installed and configured from scratch. These templates are also known as so-called ''golden images'' and aim to increase the degree of automation. In this regard, it is also relevant if customers can create their own system templates for training use.

Then, it was examined whether automation is utilised in order to create the training infrastructure. This ''training infrastructure setup automation'' describes that the systems and the network of a training environment are created. For example, VMs are deployed and configured to the point where hostnames and IP addresses are assigned, but services, client software or user administration are not yet configured, or only as basic as possible.

The next question addressed the system and network orchestration, which, in contrast to training infrastructure setup automation, is used to configure training environments, covering system-level services, software, user setup, and simulated actions. The final question asked whether widespread, freely available orchestration tools such as Ansible, Chef, or Puppet can be used. These tools offer broad community support and documentation, making it easier to adopt and customise the platform.

C. CYBER RANGE DESCRIPTION MODEL

As outlined above, the accessibility of CRs is composed of various dimensions such as platform access, training content, supervision, software architecture, scenario building,

evaluation, and ease of setup. Several features within these categories are needed to describe a CR's capabilities. Deriving from the ECSO questionnaire and our extension to it, in Section II we identified 39 questions that cover the accessibility of a CR. These were used to craft our questionnaire, which depicts all the features that allow to capture a detailed picture of a CR. To visualise these features and to allow getting an overview of which features describe a CR, we created the CR feature ontology in Fig. 1.

We chose the ontology format, as in information science, an ontology is a structured representation of data, concepts or entities, giving a formal view on their categories, properties, and relationships within a particular domain. It defines key terms and how they interconnect, providing a clear framework for organising and interpreting information [34].

For our CR feature ontology, we used the eight accessibility categories and mapped the specific CR features to these categories. This includes subcategories like *Documentation* (see Jacquette [34]) which have to be distinguished again (here 'Documentation of the CR platform' and 'Documentation of the scenario orchestration process'). We depicted these levels up to the point where answer options from expert interviews or similar would have had to be included, which would have meant representing subsets that are incomplete. This was our stopping point, as only complete subsets should be included in the ontology. We then related the features and sub-features that have dependencies, e.g., represented by dashed lines or arrows. Thus, the CR feature ontology is basically a structured representation of our questionnaire abstracting the sequence of questions. Instead, it enables to get an overview of the features that encompass a CR platform. Hence, it can be used to evaluate CRs according to existing best practices, technical trends and lessons learned from current research.

D. COMPARISON WITH PREVIOUS RESEARCH

In this section, we compare the scope, methodological approaches, and resulting dataset of our study with previous and related surveys. Our study not only provides a broader and more current overview of the CR landscape but also addresses several long-standing gaps identified in the literature.

Once the questionnaire had been crafted, our survey was conducted between August 2024 and mid-November 2024. Responsible contacts for each CR were identified via academic networks, research-project partners, CR provider websites, GitHub pages, or media reports. Initial inquiries were sent by email. Following Chowdhury et al. [27], responses were monitored to improve the response rate. If no reply was received within four weeks, alternative contacts were sought and a reminder was sent. A final follow-up was issued four weeks later to non-respondents.

In total, 41 CRs completed the questionnaire during the survey period. Five platforms had ceased operation or were no longer available, and one (DECIDE by Nuari [35]) was excluded as the provider stated that it does not really offer full CR capabilities. Four CRs agreed to participate but did not submit responses in time. Seven declined participation, and 20 did not respond despite follow-up attempts. In total, 31 CRs did not participate, and six were excluded; details and reasons are listed in the appendix in Table 24. Nevertheless, we were able to receive data from a representative set of CRs, which allows us to also draw conclusions about the current CR landscape.

1) SCOPE AND COVERAGE OF CYBER RANGES

Compared to prior work (see Section III), our study analyses 41 CRs in detail, with feature-level data collected directly from platform providers. This enables a significantly more comprehensive and up-to-date overview of existing CR platforms. While earlier surveys such as Davis and Magrath [8], Leblanc et al. [9], and Holm et al. [21] focused either on a limited number of platforms or broader categories such as simulation testbeds and ICS-specific environments, we exclusively examine CRs as defined in current discourse and fill data gaps left by earlier studies, such as Ukwandu et al. [10].

Yamin et al. conducted a systematic literature review and identified 100 relevant publications but only included data on CRs already described in scientific papers [7]. Consequently, many commercial or operational platforms remained underrepresented. In contrast, our direct outreach allowed the inclusion of both academic and industry/government CRs, capturing features and technologies not previously documented.

2) METHODOLOGICAL EVALUATION

Unlike earlier studies that relied mainly on literature reviews and lacked consistent CR taxonomies, our study combines a systematic literature review with a structured survey based on a detailed CR feature ontology. While Davis and Magrath grouped CRs broadly by simulation type [8] and Leblanc et al. focused on cyberattack simulation approaches [9] the term 'Cyber Range' itself was still emerging. Holm et al. [21] utilised a structured review combined with a taxonomy but with a clear focus on ICS testbeds, while Ukwandu et al. [10] also conducted a structured review, but did not apply the taxonomy they developed to the CRs they studied.

In contrast, our ontology enables fine-grained comparison of CR capabilities. Compared to Yamin et al. [7], who developed a broader, also management-oriented taxonomy that targets the processes for providing a CR platform, our approach captures structural feature relationships and enables a fine-grained comparison of platform capabilities. While Chouliaras et al. [11] gathered data from 10 CRs via interviews, our survey covers four times as many platforms and collects richer data, enabling more robust trend analysis.

3) TAXONOMIES AND FEATURE COMPARISONS

Yamin et al. [7] proposed a broad taxonomy including scenario management and platform operations, but did not

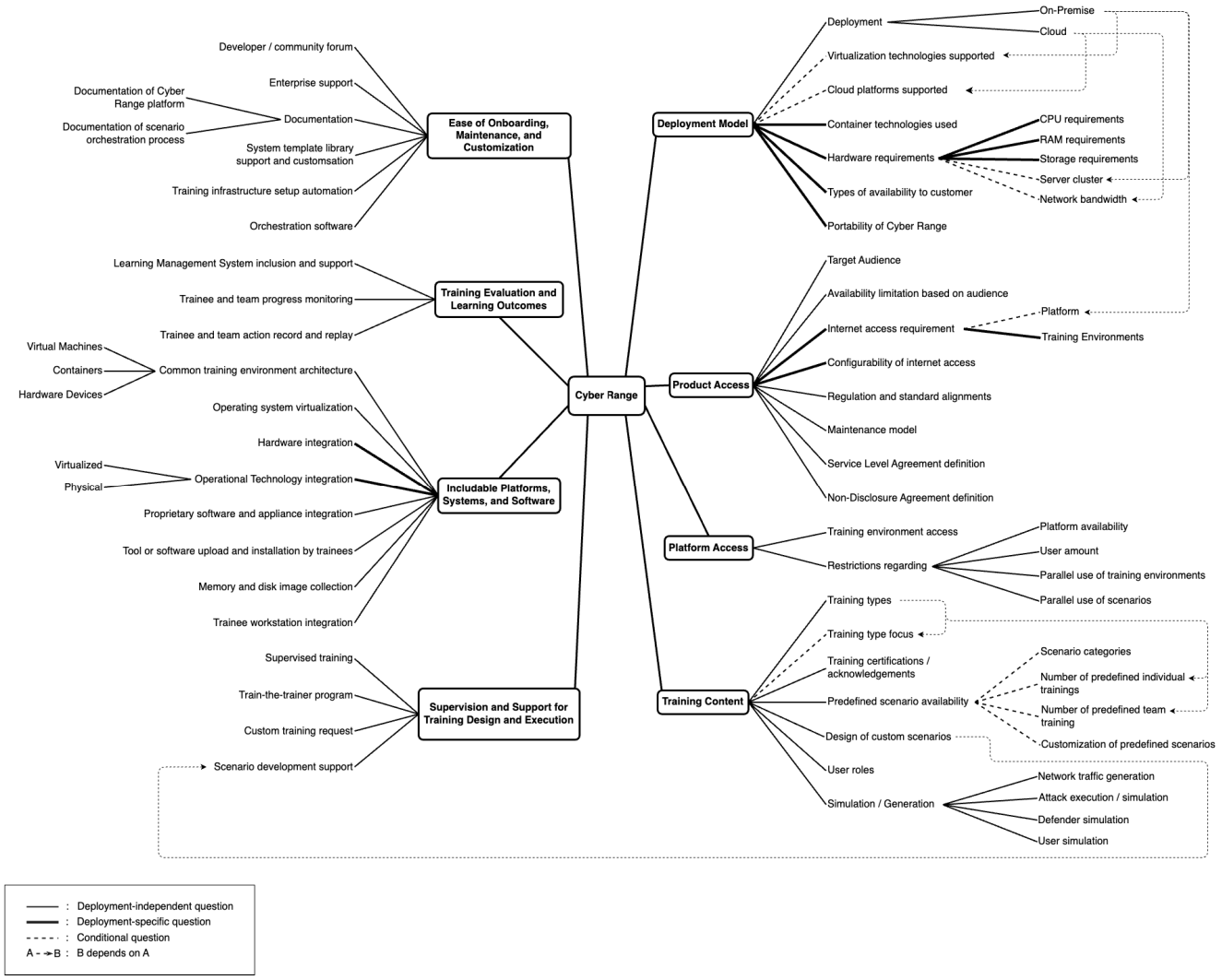


FIGURE 1. Cyber range feature matrix.

include structural relationships between features. Their tool listings, based solely on literature, do not indicate tool adoption, prevalence or in which contexts tools are deployed, and primarily reflect CR platforms from academic and research contexts. As a result, there is a lack of actual data on platforms from the industry or government sectors. Our study, by contrast, provides insights into which tools are most frequently used for key functionalities such as virtualisation, simulation, automation, user simulation, and monitoring based on CR provider input.

Furthermore, while Yamin et al. [7] outlined a wide range of tools used in CRs, including emulation, simulation, monitoring, and traffic generation tools, their classification often mixes different abstraction levels – for example, grouping virtualisation platforms (e.g., KVM, VMware), management frameworks (e.g., Proxmox, OpenStack), and components (e.g., OpenFlow Switches) together. We distinguish between these layers, enabling clearer insights into tool adoption in the field.

Yamin et al. offer a broad catalogue of simulation and user generation tools [7]. However, our data – based on direct input from commercial CR operators – provides a more focused and usage-oriented view. On hardware integration, Yamin et al. [7] list specific devices; we assess the integration capabilities of platforms more generally, offering complementary insights.

Ukwandu et al. [10] list many platforms but lack quality appraisal, leading to a mix of CRs and general testbeds. Additionally, it remains unclear whether all listed platforms are still operational. Their comparison table reveals major data gaps, particularly regarding the technology stack, tool usage, and training capabilities. Crucially, neither automation technologies nor the actual training content are covered. Although a taxonomy is introduced later in their study,

TABLE 1. Comparison of cyber range surveys.

Article	Sources	Included Platforms	Actuality	Cyber Range specific Focus	Comprehensive Cyber Range Feature Analysis	Cyber Range specific Classification Scheme applied	Comprehensive Detail Data on Cyber Ranges
Leblanc et al. [9]	Mixed literature review	13	2011	×	×	×	×
Davis and Magrath [8]	Mixed literature review	30	2013	✓	×	✓	×
Holm et al. [21]	Scientific literature review	30	2015	×	×	×	×
Yamin et al. [7]	Scientific literature review	N/A	2018	✓	✓	✓	×
Ukwandu et al. [10]	Scientific literature review	44	2020	✓	✓	×	×
Chouliaras et al. [11]	Scientific literature review + Structured Interviews	10	2021	✓	×	×	✓
Steiner et al. [12]	Mixed literature review + Two Case Studies	15	2022	✓	×	×	×
Lazarov et al. [13]	Mixed literature review	35	2023	×	×	×	×
Our research	Mixed literature review + Structured Questionnaire	41	2025	✓	✓	✓	✓

✓ = Yes, × = No, N/A = Not directly specified

it was not used to structure the feature data from the outset, resulting in an incomplete and only limited comparison of CR features. Our study addresses these issues through a structured, ontology-based approach and provider-sourced data.

Table 1 shows a comparison of our research and the related work. The scientific methodology, scope, up-to-dateness, extent and comprehensiveness of the individual studies are presented as an overview. The 'Sources' column distinguishes between purely *scientific literature reviews* and *mixed literature reviews*, which also include additional sources from the private sector, academia & research, and military & government. It also notes whether empirical methods (e.g., questionnaires, interviews, case studies) supplement these. 'Included Platforms' refers to the number of platforms considered (if reported), without assessing completeness or CR-specificity. Therefore, 'CR specific focus' indicates whether the study focuses on CRs. 'Comprehensive CR Feature Analysis' shows whether CR features were thoroughly identified and described – possibly forming the basis for a taxonomy. 'CR specific Classification Scheme applied' then indicates whether such a taxonomy or ontology was used to compare CRs. Finally, 'Comprehensive Detail Data on CRs' reflects whether detailed data on the CRs under consideration was provided, enabling comparison or an overview of the CR landscape.

V. RESULTS OF THE SURVEY

The answers in the questionnaires included both quantitative and qualitative data. Qualitative responses were standardised for comparison. However, all raw responses are available on the Open Data UniBw M platform of the University of the Bundeswehr Munich.[1] This open-access repository is based on the Dataverse platform. For analysis, we developed a web-based tool that allows filtering questionnaire data by (i) CR, (ii) survey question, or (iii) keyword search. To enhance accessibility for the public and enable future updates or additions, this "CR search engine" was published as a freely available website.[2] In the following, we present our survey results across 21 tables, dedicated to the eight different accessibility categories plus one table summarising the general information about each CR.

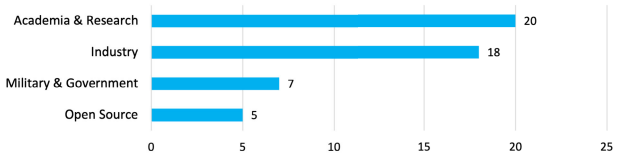


FIGURE 2. Cyber ranges proficiency sectors (N = 41).

A. GENERAL INFORMATION ABOUT PARTICIPATING CYBER RANGES

First, Table 2 shows general information about each CR, including the affiliated organisation responsible for its development, provision, or distribution. Based on this affiliation, one or more of the following sectors are assigned: *Academia & Research*, *Military & Government*, *Industry*, and *Open Source*. While the first three are commonly used, the Open Source category was included to cover platforms like the Vigrid CR that do not fit into these traditional sectors. Some CRs, such as Vigrid, are provided under an Open Source license and this should be recognisable from our data. If applicable, multiple sectors were assigned to a CR provider to reflect hybrid affiliations. For instance, the Swedish Defence Research Agency (FOI), which provides CRATE, conducts research and is subordinate to the Ministry of Defence [82].

[1] https://doi.org/10.60776/F1WOHD

[2] https://go.unibw.de/cyber-range-comparison

TABLE 2. Cyber range general platform information.

Cyber Range	Affiliation	Sector	Development
AIT Cyber Range [13], [15], [36]–[41]	Austrian Institute of Technology (AIT) GmbH	Academia & Research, Industry	In-house Development
Airbus CyberRange [13], [15], [39], [42]–[45]	Airbus Defence And Space GmbH	Industry	In-house Development
Brno University of Technology Cyber Arena (BUTCA) [13], [46]	Brno University of Technology	Academia & Research	In-house Development
Cyber Defence eXercise Platform (CDeX) [15], [43]	CDeX	Industry	In-house Development
Coliseum [15]	Nortal AS	Industry	In-house Development
CRACK aka ARTIC Cyber Range [15], [44]	Universita Degli Studi di Genova	Academia & Research	In-house Development
Cyber Range And Training Environment (CRATE) [13], [37], [38], [44], [47]–[52]	Swedish Defense Research Agency (FOI)	Military & Government, Academia & Research	In-house Development
Cybels Train and Experiment (Cybels) [15], [53]	Thales Deutschland GmbH	Industry	In-house Development
Immersive Cyber Range Exercising (Immersive) / formerly Team Sim [54]	Immersive Labs	Industry	In-house Development
Cyber Simulation Center [15]	Hensoldt AG / formerly ESG	Industry	Customised: Initially implemented with IAI TAME Range, gradually replaced by own solutions
Cyberbit Range [12], [13], [39], [40], [44], [49], [55]–[57]	Cyberbit GmbH	Industry	In-house Development
Cyberoperations Enhanced Network & Training Simulators (CENTS) + RangeOS [39], [56]	CyberCENTS & By Light Professional IT Services LLC	Industry	In-house Development
Cybermentis [15]	CYS4	Industry	In-house Development
TELECOM Nancy Cyber Range [25]	University of Lorraine & TELECOM Nancy	Academia & Research	Customised: Diateam Cyber-Range + Airbus Defense and Space Cyber Cyber-Range
CybExer Cyber Range [13], [15], [39], [49]	CybExer	Industry	In-house Development
Cyber Security Operations Platform (CySOP) [49], [58]	Keysight	Industry	In-house Development
Cyrange / formerly Cylab [13], [59]	Royal Military Academy	Military & Government, Academia & Research	In-house Development
CYRIN [49]	ATC-NY	Industry	In-house Development
CyTrONE [26], [38], [41], [60]–[64]	Japan Advanced Institute of Science and Technology (JAIST)	Academia & Research, Open Source	In-house Development
DIATEAM Hybrid Cyber Range / formerly HNS Platform [15], [39], [43], [49], [65]	DIATEAM	Industry	In-house Development
EDURange [12], [15], [41], [61], [63]	Evergreen State College	Academia & Research, Open Source	In-house Development
IT Competence Education & Training (ICE&T) Cyber Range [66]	Research Institute (RI) CODE	Academia & Research, Military & Government	Customised: TAME Range By IAI
iTrust Labs [67]	iTrust &s Singapore University of Technology and Design	Academia & Research, Military & Government	In-house Development
KYPO Cyber Range Platform (KYPO CRP) [13], [15], [26], [38]–[41], [44], [58], [61]	Masaryk University & CybersecurityHubCZ	Academia & Research, Open Source	In-house Development
Laokoon Attack Xperience [68]	Laokoon Security GmbH	Industry	In-house Development
Luxembourg Cyber Range [69]	Luxembourg Directorate of Defense (LDoD)	Military & Government	Customised: proprietary product; concrete platform cannot be stated due to LDoD internal restrictions
Maine Cyber Range (MCR) [56]	University of Maine at Augusta	Academia & Research	Customised: Cyberbit Range
M&NTIS Platform [15]	AMOSSYS	Industry	In-house Development
Mizzou Cyber Range [70]	University of Missouri-Columbia	Academia & Research	In-house Development
Ohio Cyber Range [56], [71]	Ohio Cyber Range Institute (OCRI) at the University of Cincinnati	Academia & Research	Customised: VMWare VRealize Automation/VCenter
Open Cyber Range (OCR) [13], [37], [38], [49], [58], [72]	Foundation CR14	Military & Government, Open Source	In-house Development
PAIDEUSIS [15]	CINI - Cybersecurity National Lab	Academia & Research	In-house Development
Range365 [13]	Cloud Range	Industry	In-house Development
RangeForce Cyber Readiness Platform [12], [13]	RangeForce	Industry	In-house Development
Realistic Global Cyber Environment (RGCE) [13], [15], [39], [73], [74]	JYVSECTEC by Jamk University of Applied Sciences	Academia & Research	In-house Development
SimSpace Platform / formerly Ravello [43], [49]	SimSpace Corporation	Industry	In-house Development
SPHERE / formerly DETERLab [15], [20], [38], [49], [61], [62], [70], [75]–[79]	USC Information Sciences Institute	Academia & Research	In-house Development
Tecnalia Cyber Range Laboratory [15]	Tecnalia Research & Innovation	Academia & Research	In-house Development
UNSW Cyber Range [80]	University of New South Wales (UNSW) Canberra	Academia & Research, Military & Government	Customised: Combination In-house / Skillable Online Cloud
Vigrid [15]	None	Open Source	In-house Development
Virginia Cyber Range aka U.S. Cyber Range of Virginia Tech [13], [37], [39], [40], [49], [56], [57], [81]	Virginia Polytechnic Institute and State University	Academia & Research	In-house Development

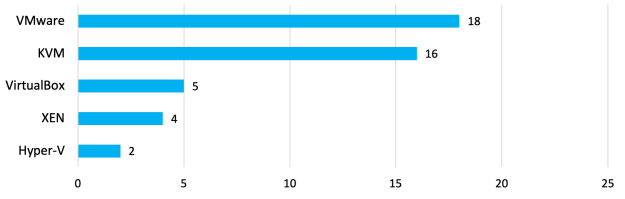


FIGURE 3. Supported virtualisation technologies (N = 33).

Table 2 also lists all full names, former names, and acronyms of the participating CRs in the column 'Cyber Range'. In the text and the following tables, only acronyms are used (if available). Sources from which CRs were identified during the literature review are included in the table, but are omitted in the following tables and text for the sake of simplicity and readability. The column 'Development' shows how each CR was set up. The option *Purchased and used without customisation* was not selected by any of the survey participants. This can be interpreted as confirmation that CR platforms need to be highly adapted to the needs of the customers.

Of the 41 participants, 34 developed their CR in-house, while seven customised purchased products. Notably, five

TABLE 3. Cyber range deployment model features.

Cyber Range	On-Premise Product						Cloud Product					
	Virtualisation	Container Deployment	CPU	RAM	Storage	Cluster	Cloud Platforms	Container Deployment	CPU	RAM	Storage	Band-width
AIT Cyber Range	KVM, OpenStack	Docker	L	XL	L	✓	AWS, Google Cloud, Azure, Private Cloud, OVH	Docker	XL	XL	XL	XL
Airbus CyberRange	VMware	×	M	M	S	×	Private Cloud, other clouds possible with additional effort	×	M	M	S	S
CDeX	OpenStack	Docker	M	L	XL	×	AWS, Azure	Docker	XL	L	XL	XL
Coliseum	VMware	Docker	L	L	L	×	All that allow VMWare deployment	Docker	L	L	L	S
CRACK	KVM	podman	S	S	S	×	–	–	–	–	–	–
CRATE	KVM, Virtual Box	Docker, Lxc	M	L	L	✓	–	–	–	–	–	–
CYRIN	KVM, OpenStack	×	M	M	L	×	Azure, Private Cloud	×	M	M	L	S
CySOP	Proxmox VE	×	M	M	L	×	–	–	–	–	–	–
CyTrONE	KVM	×	S	S	S	×	AWS	×	S	S	S	×
CybExer Cyber Range	VMware	Docker	M	XL	XL	✓	AWS, Azure, Google Cloud, Private Cloud	Docker	S	S	S	×
Cybels	Proxmox	Docker	XL	L	L	✓	–	–	–	–	–	–
UNSW Cyber Range	VMware, Proxmox (in testing)	Docker, Lxc	L	XL	XL	✓	Skillable	Docker	M	M	L	×
Immersive	–	–	–	–	–	–	AWS	×	S	S	L	M
Cyber Simulation Center	VMware	×	M	L	L	✓	–	–	–	–	–	–
CENTS + RangeOS	KVM	Docker, Lxc	N/A	N/A	N/A	N/A	Universal platform support	Docker	N/A	N/A	N/A	N/A
Cyberbit Range	VMware	×	M	L	L	×	AWS, Azure	Docker	M	L	L	×
Cybermentis	–	–	–	–	–	–	AWS	Docker	N/A	N/A	N/A	N/A
TELECOM Nancy Cyber Range	VMware, KVM	Docker	XL	XL	XL	✓	–	–	–	–	–	–
Cyrange	Virtual Box	Docker	S	S	S	×	–	–	–	–	–	–
DIATEAM Hybrid Cyber Range	KVM, QEMU	Lxc	L	L	L	×	–	–	–	–	–	–
EDURange	VMware, Virtual Box	Docker	S	S	M	×	AWS, Google Cloud	Docker	S	M	M	S
ICE&T	VMware	×	XL	XL	XL	✓	–	–	–	–	–	–
iTrust Labs	VMware, Hyper-V, Virtual Box	Docker in certain cases	L	XL	L	✓	Cloud at the National University of Singapore R&D Cybersecurity Lab	Docker in certain cases	XL	XL	XL	M
BUTCA	–	–	–	–	–	–	Private Cloud	Lxc	XL	XL	XL	S
KYPO CRP	–	–	–	–	–	–	AWS, Private Cloud	Docker	M	L	M	S
Laokoon Attack XPerience	VMware, Hyper-V	Kubernetes, Docker	L	L	M	N/A	AWS, Private Cloud	Kuberentes, Docker	M	L	M	N/A
Luxembourg Cyber Range	VMware	Docker	L	XL	XL	✓	–	–	–	–	–	–
M&NTIS Platform	KVM	Docker	M	L	M	N/A	Scaleway	Docker	M	M	M	S
MCR	VMware	×	M	L	L	×	–	–	–	–	–	–
Mizzou Cyber Range	–	–	–	–	–	–	Google Cloud	Docker	S	S	S	×
Ohio Cyber Range	VMware	×	XL	XL	XL	✓	–	–	–	–	–	–
OCR	VMware, OpenStack	Docker	M	S	S	N/A	–	–	–	–	–	–
PAIDEUSIS	KVM	Docker	M	M	L	×	–	–	–	–	–	–
Range365	–	–	–	–	–	–	Google Cloud	×	M	L	M	×
RangeForce Cyber Readiness Platform	–	–	–	–	–	–	AWS, Azure, Google Cloud, Private Cloud	Docker	XL	XL	XL	L
RGCE	VMware	Docker, Lxc, Kubernetes	XL	XL	XL	✓	–	–	–	–	–	–
SPHERE	KVM	Kubernetes	XL	XL	S	✓	–	–	–	–	–	–
SimSpace Platform	VMware	Docker	XL	XL	L	N/A	Private Cloud, self owned datacenter	Docker	S	S	S	×
Tecnalia Cyber Range Laboratory	VMware, Virtual Box	×	XL	XL	XL	✓	–	–	–	–	–	–
Vigrid	QEMU managed by GNS3	Docker	S	S	S	×	–	–	–	–	–	–
Virginia Cyber Range	–	–	–	–	–	–	AWS	Docker, AWS Fargate & ECS	S	S	S	S

✓ = Required × = No requirement/Not used, N/A = No information provided, – = No on-premise or cloud product

of the latter are from the academia & research sector: the University of Lorraine & TELECOM Nancy, the Research Institute (RI) CODE, the University of Maine, the Ohio Cyber Range Institute (OCRI), and the University of New South Wales (UNSW) Canberra. The RI CODE and the UNSW Canberra, however, also have a link to military & government [83], [84]. The Luxembourg Cyber Range (military) and Hensoldt AG's Cyber Simulation Center (industry) are also based on purchased products, suggesting a focus on training – confirmed in Table 3.

Five CRs are affiliated with both academia & research and military & government. This leads to the conclusion that CR platforms are particularly relevant in research and educational activities related to government and military services. Overall, however, most participants developed their CRs on their own. Fig. 2 summarises the sector affiliations.

B. RESULTS REGARDING DEPLOYMENT

Table 3 shows the hardware and virtualisation features that were asked regarding the accessibility category 'Deployment Model'. This concerns the deployment or setup options for a CR platform but also the necessary hardware resources.

1) DEPLOYMENT MODELS

This subcategory targets the deployment models, virtualisation technologies, and cloud providers of the CRs. Table 3 shows that 33 CRs are (or can be) deployed on-premise if the platform is offered as a product. Among them, 11 support

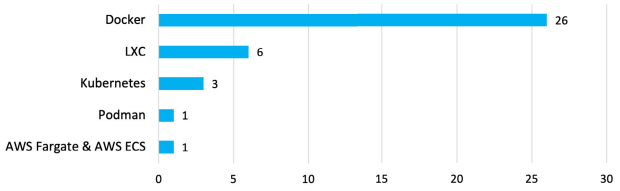


FIGURE 4. Supported container technology (N = 31).

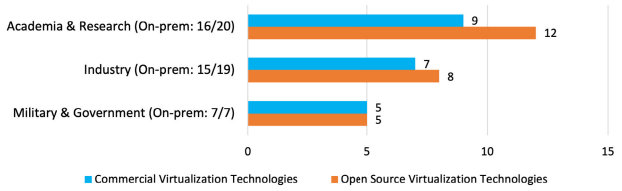


FIGURE 5. Cyber range on-premise virtualisation technology (N = 38).

KVM, 18 VMware, five VirtualBox, and two Hyper-V. Although XenServer was listed, none selected it directly. However, four mentioned OpenStack – an Open Source cloud computing infrastructure [85] – in free-text responses. As OpenStack basically requires KVM or XenServer as hypervisors [86], all four were counted as supporting both. Similarly, Proxmox Virtual Environment (mentioned three times) – an Open Source server management and virtualisation platform – is tied to KVM [87] and has been treated accordingly.

Two other solutions – QEMU and GNS3 – were also named. QEMU is an Open Source machine emulator and virtualiser. It supports virtualisation when used in conjunction with XenServer or KVM [88]. GNS3 is a network emulator that allows to combine virtual and physical devices to simulate complex networks [89]. Fig. 3 summarises virtualisation support, excluding emulators.

Container usage was confirmed by 23 on-premise CRs: 20 use Docker, five LXC, and one Podman (named by the CRACK CR). Furthermore, Kubernetes was named by Laokoon Attack XPerience, RGCE, and SPHERE. It is an Open Source container management application that supports numerous container runtimes including Docker, containerd, CRI-O, and any implementation of the Kubernetes CRI (Container Runtime Interface) [90].

Beyond on-premise setups, 23 CRs can be deployed or are offered in the cloud. Providers reported support for AWS (14), Azure (8), Google Cloud (8), private/in-house clouds (11), and other platforms (e.g., OVH, Skillable, Scaleway). Five state to be operational with basically any cloud platform (e.g., Coliseum via VMware). Eigthteen of these cloud-deployed CRs support or use container technologies for platform deployment: 17 support Docker, BUTCA supports LXC, Laokoon uses Kubernetes, and the Virginia CR uses AWS Fargate/ECS. A total of 15 CRs support both on-premise and cloud deployment. Fig. 4 presents container technologies used across all setups, counting each CR only once. With the exception of BUTCA, Docker is always supported by the cloud-based CRs that support or use a container technology for their deployment.

All participating CRs use virtualisation – either directly or through cloud services. No platform reported a non-virtualised deployment, although we offered this answer option. From this, it can be concluded that virtualisation is the dominant underlying technology for CRs. Purely hardware-based CRs can be seen as exceptions. Thereby, VMware and KVM are dominant (see Fig. 3), while XenServer, despite being OpenStack-compatible, is not commonly used.

In total, 31 of 41 CRs use or support container technologies in the provisioning of their platform, with Docker being by far the most prevalent. However, Container use is slightly more common in cloud setups (78%) than on-premise (70%). It is worth noting that providers that offer both cloud and on-premise CRs do not necessarily use container technologies in both setups, nor do all support or use the same container technologies consistently in both environments. Differences exist, for example, with the Cyberbit Range, CENTS + Range OS, or the UNSW CR.

Fig. 5 explores the relationship between the operator sectors from Table 2 and the supported virtualisation platforms for on-premise deployments. Additionally, it shows how many CR providers in each sector offer an on-premise CR. Somewhat surprisingly, the operator's sector does not influence the type of virtualisation platform used. In the industry sector, Open Source solutions like KVM and XenServer are supported about as often as enterprise products (e.g., VMware or Hyper-V). In academia & research, support for both platform types is similarly balanced – even when excluding CRs based on customised commercial products. The Luxembourg CR, the only exclusively military CR in our dataset, uses VMware. Interestingly, however, all participating platforms assigned to the military sector are available on-premise. In all other sectors, the form of availability varies (see Table 3).

While all industry CRs from our set use only a single virtualisation solution – either enterprise or Open Source – academia & research CRs often support both. In the military & government sector, a balanced use is observed, though conclusions are limited due to low participation.

2) RESOURCE REQUIREMENTS

As specifying hardware requirements was optional, some CRs (e.g., CENTS + RangeOS) provided no information on on-premise or cloud setups, cluster use, or bandwidth needs. To standardise responses, CPU, RAM, storage, and network requirements were categorised into four levels: *S*, *M*, *L*, and *XL*, as shown in Table 3, Fig. 6, and Fig. 7.

For CPUs, S = 1-16 cores, M = 17-64, L = 65-128, and $XL \geq 128$. For RAM requirements, 1-64 GB corresponds to

TABLE 4. Cyber range availability types.

Cyber Range	Customers' Server	Customers' Cloud	Ready to Use	Web	VPN	Training Center	Mobile	Supplementary information
AIT Cyber Range	✓	✓	✓	✓	×	✓	off-the-shelf	–
Airbus CyberRange	×	×	✓	✓	✓	✓	off-the-shelf	–
CDeX	✓	✓	✓	✓	✓	✓	off-the-shelf	–
Coliseum	✓	✓	✓	✓	✓	✓	self deployment	–
CRACK	×	×	×	✓	✓	×	self deployment	–
CRATE	✓	×	✓	✓	✓	×	self deployment	–
CYRIN	✓	×	×	✓	×	×	self deployment	–
CySOP	✓	×	×	×	×	×	self deployment	may be prepackaged by a reseller
CyTrONE	✓	✓	×	×	×	×	self deployment	Open Source
CybExer Cyber Range	✓	✓	✓	✓	✓	✓	off-the-shelf	–
Cybels	×	×	×	✓	×	✓	×	–
UNSW Cyber Range	×	×	×	✓	✓	✓	×	–
Immersive	×	×	×	✓	✓	×	×	–
Cyber Simulation Center	×	×	×	×	✓	×	×	–
CENTS + RangeOS	×	✓	✓	×	✓	×	off-the-shelf	–
Cyberbit Range	×	×	✓	✓	✓	×	self deployment	–
Cybermentis	×	×	×	✓	×	×	×	–
TELECOM Nancy Cyber Range	×	×	×	✓	✓	✓	×	–
Cyrange	×	×	×	×	×	✓	self deployment	currently only self-use
DIATEAM Hybrid Cyber Range	×	×	✓	×	✓	✓	off-the-shelf	–
EDURange	✓	✓	×	✓	×	×	self deployment	–
ICE&T	×	×	×	×	×	✓	×	VPN access in development
iTrust Labs	×	×	×	×	✓	✓	×	–
BUTCA	×	×	×	✓	×	×	×	–
KYPO CRP	✓	✓	×	✓	×	✓	self deployment	–
Laokoon Attack XPerience	✓	×	×	×	✓	✓	self deployment	–
Luxembourg Cyber Range	×	×	×	✓	✓	✓	×	–
M&NTIS Platform	✓	×	×	✓	×	×	self deployment	–
MCR	×	×	✓	×	✓	✓	×	–
Mizzou Cyber Range	×	×	×	✓	×	×	self deployment	–
Ohio Cyber Range	×	×	×	✓	×	✓	self deployment	–
OCR	✓	✓	×	×	✓	✓	self deployment	Open Source
PAIDEUSIS	×	×	×	✓	✓	×	×	–
Range365	×	×	×	✓	×	×	×	–
RangeForce Cyber Readiness Platform	×	×	×	✓	×	×	×	–
RGCE	×	×	×	×	✓	✓	×	–
SPHERE	×	×	×	✓	×	×	self deployment	–
SimSpace Platform	✓	×	✓	✓	×	×	self deployment	–
Tecnalia Cyber Range Laboratory	×	×	×	×	✓	✓	×	Through public-subdomains and a reverse proxy
Vigrid	✓	×	×	×	×	×	self deployment	Open Source, User2LAN & LAN2LAN access
Virginia Cyber Range	×	×	×	✓	×	×	×	–

✓ = Method available × = Method not available, – = No supplementary information

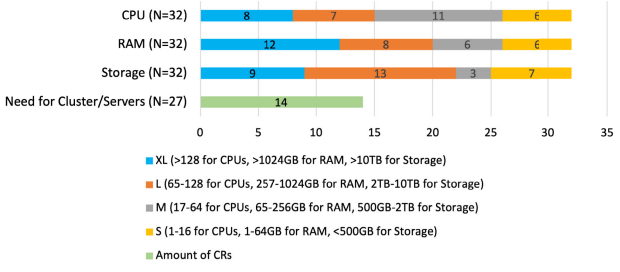


FIGURE 6. Required resources on-premise.

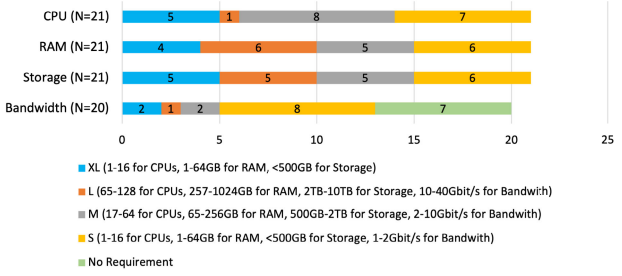


FIGURE 7. Required resources cloud.

S, 65-256 GB to M, 257-1024 GB to L, and $\geq$ 1024 GB to XL. For the storage requirements, S means < 500 GB, M < 2TB, L < 10 TB, and XL to any size larger than 10 TB. For network bandwidth, you could specify that there is no such requirement. Otherwise, S represents a maximum possible data transfer rate of 1-2 Gbit/s, M = 2-10 Gbit/s, L = 10-40 Gbit/s, and $XL \geq$ 40 Gbit/s.

Usable data was provided by 32 of 33 on-premise CRs. The results are summarised in Fig. 6, for cloud-deployed CRs see Fig. 7. Among on-premise CRs, low requirements (S) in

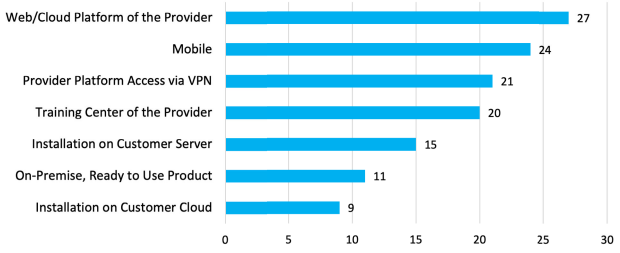


FIGURE 8. Types of availability (N = 41).

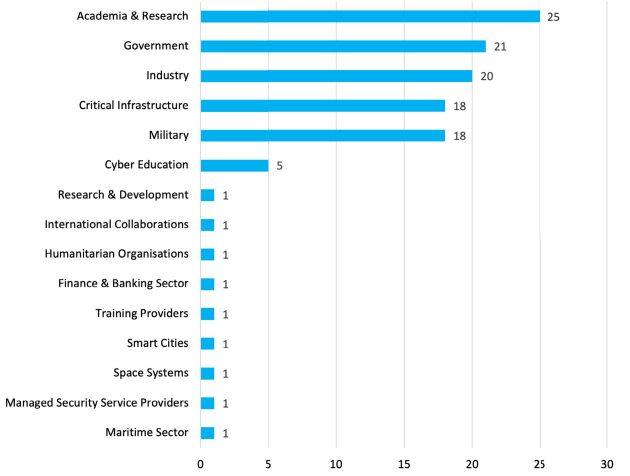


FIGURE 9. Cyber range focus areas (N = 29).

one category often coincide with low requirements in others. CRACK, CyTrONE, Cyrange, and Vigrid have *S*-level needs throughout; EDURange and CR14's Open Cyber Range show only one *M*-level value. All are linked to Open Source or academia & research, suggesting platforms for research or demonstration demand fewer resources. Exceptions include SPHERE and the Airbus CyberRange, with overall high needs but *S*-level storage.

In contrast, CRs that are not designed for minimal hardware utilisation often show significantly higher demands. Multi-server or cluster deployment is required by 14 platforms and many exhibit *XL*-level RAM requirements. Most CRs need *L*-level storage and *M*-level CPU.

Cloud-based CRs generally require fewer resources. Eight of 21 platforms report only *S*- or *M*-level needs in all queried categories (see Table 3). Additionally, there are CRs, such as Immersive, which e.g., requires only *S* for CPU and RAM but *L* for storage. However, lower requirements in the cloud do not correlate strongly with academic affiliation but reflect cloud scalability. Still, several cloud CRs also show high to very high demands, similar to on-premise counterparts. An interesting point to note, however, is that just because a provider offers both a cloud and an on-premise CR, this does not imply identical resource requirements.

3) AVAILABILITY TYPES

Table 4 depicts the general availability types of CR platforms for customers (not trainees), including additional comments in the *Supplementary Information* column. Fig. 8 quantifies how many CRs support each type.

Of the 41 platforms, 20 are offered as installable products – on customer servers, cloud environments, or as preconfigured, ready-to-use systems – implying a product-oriented business model. However, five of these are Open Source and thus not sold commercially, leaving 15 platforms classified as CR vendors.

CyTrONE, Vigrid, and CySOP are only available as installable platforms without training-as-a-service. In contrast to CyTrONE and Vigrid, the other Open Source CRs also offer training: OCR via training centre/VPN, KYPO CRP and EDURange via web access or training centre.

With 38 platforms that offer access via the provider's infrastructure-VPN, web/cloud platform, or training centre, the majority of our participants is training-oriented. Of these, 21 offer no installable version and provide training access only. ICE&T and Cyrange are only accessible on-site at their training centre. Both belong to academia & research with military links, suggesting restricted access due to institutional background. There are 36 CRs that support remote training via web, cloud, or VPN. Seven of these are pure cloud providers (e.g., RangeForce, SPHERE, BUTCA). Interestingly, however, four of them are linked with academia & research rather than industry.

Among the 20 CR platform-focused providers, only KYPO requires cloud deployment (see Table 3). However, this includes the private cloud and thus enables a deployment with OpenStack and thereby KVM, or XenServer. Of the remaining 19, nine support enterprise virtualisation and 12 support Open Source, without clear preference. Even regarding CR platform vendors that offer their platform either commercially or Open Source, no clear dominance of enterprise virtualisation platforms can be deduced.

Of the 21 pure training providers, seven require cloud deployment, only three support private cloud, and only BUTCA explicitly requires it. Private cloud deployment is supported by 11 of 23 cloud-deployed CRs, but just four require it. Most support commercial cloud platforms, which shows that it is not necessarily prioritised that all data remains on the company's own infrastructure during CR training.

Considering only platforms that offer access exclusively via the web/cloud (see Table 4), four of six rely solely on commercial clouds. Only SPHERE is fully self-hosted on KVM. This aligns with cost-efficient scaling via shared infrastructure in the cloud.

A majority of 14 of the 21 training-focused CR providers is from academia & research. This indicates a focus on internal training (e.g., students). Five of seven military CRs follow the same model. By contrast, only six of 18 industry CRs are pure training providers.

TABLE 5. Cyber range access and focus groups.

Cyber Range	Provider Sector	Focus Group	Limited To
ICE&T	Academia & Research, Military & Government	×	Access is only available in consultation with RI CODE
CySOP	Industry	×	×
Immersive	Industry	×	×
iTrust Labs	Academia & Research, Military & Government	Military, Government, Critical Infrastructure, Academia & Research, Industry, For cyber exercises in particular	Military, Government, Critical Infrastructure, Academia & Research, Industry, Depends on context of the request
TELECOM Nancy Cyber Range	Academia & Research	Academia & Research, Industry	×
Vigrid	Open Source	×	×
SPHERE	Academia & Research	Government	Government
CENTS + RangeOS	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
Laokoon Attack XPerience	Industry	Military, Government, Critical Infrastructure, Industry	Military, Governmental entities, and Industry of NATO member states
MCR	Academia & Research	×	×
KYPO CRP	Academia & Research, Open Source	Government, Critical Infrastructure, Academia & Research, Industry	Commercial services/support provided only to organisations from EU/NATO member states
Cyber Simulation Center	Industry	Military, Government, Critical Infrastructure	×
Cyrange	Academia & Research, Military & Government	Academia & Research	Early BETA, so for testers only
EDURange	Academia & Research, Open Source	×	×
Virginia Cyber Range	Academia & Research	Educators in high school, community colleges, and universities	×
CRATE	Academia & Research, Military & Government	×	Military, Government, Critical Infrastructure, Academia & Research
RGCE	Academia & Research	Military, Government, Critical Infrastructure, Academia & Research, Industry, R&D Projects and International collaboration	×
BUTCA	Academia & Research	Military, Government, Critical Infrastructure, Academia & Research, Industry, Students & Public	×
OCR	Open Source, Military & Government	×	×
Luxembourg Cyber Range	Military & Government	Military, Government, Critical Infrastructure, Academia & Research, humanitarian organisations	Military, Government, Critical Infrastructure, Academia & Research, humanitarian organisations
PAIDEUSIS	Academia & Research	×	×
Tecnalia Cyber Range Laboratory	Academia & Research	Academia & Research	×
Airbus CyberRange	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry, Schools, E-Learning	×
M&NTIS Platform	Industry	Military, Government, Academia & Research, Industry	×
CYRIN	Industry	×	×
Range365	Industry	×	×
CyTrONE	Academia & Research, Open Source	×	×
Cybermentis	Industry	Government, Critical Infrastructure, Academia & Research, Industry	×
RangeForce Cyber Readiness Platform	Industry	Academia & Research, Industry	Academia & Research, Industry
Cybels	Industry	Critical Infrastructure, Academia & Research, Industry	×
UNSW Cyber Range	Academia & Research, Military & Government	Military, Government, Academia & Research, Education for students	Military, Government, Academia & Research, Enrolled students
SimSpace Platform	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
CRACK	Academia & Research	Academia & Research	×
Mizzou Cyber Range	Academia & Research	Academia & Research	×
Ohio Cyber Range	Academia & Research	Military (Unclassed/CUI), Government, Academia & Research, Industry, K-12	Only available to Ohio non-profit organisations and above or at a charge to others on a project basis
Coliseum	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
DIATEAM Hybrid Cyber Range	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
CybExer Cyber Range	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry, Finance and Banking, Training Providers, Smart Cities, Space Systems, MSSPs	×
Cyberbit Range	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
AIT Cyber Range	Academia & Research, Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry	×
CDeX	Industry	Military, Government, Critical Infrastructure, Academia & Research, Industry, Maritme sector	×

× = **None**

Furthermore, all off-the-shelf, transportable CRs come from vendors and are commercially oriented. However, all non-training-only CRs can also be deployed portably. This enables the usage as mobile training units – an attractive option for large enterprises or military contexts requiring flexibility.

C. RESULTS REGARDING PRODUCT ACCESS

In this section, the results regarding the accessibility category 'Product Access' are presented. Therefore, several key areas were queried: (i) target audience and focus group based access limitations, (ii) Internet requirements and configurability, as well as (iii) maintenance, support, agreements, and alignments.

1) FOCUS AREAS AND PRODUCT ACCESS LIMITATIONS

Table 5 links the CR focus areas and access restrictions with the provider sectors. Of the 41 CRs, 29 define target groups: 25 focus on academia & research, 21 on government, 20 on industry, 18 each on military and critical infrastructure. This

broad coverage indicates that the focus groups we proposed are well covered by the CRs that have target sectors. However, while all categories are represented at similar frequencies, academia & research stands out – consistent with the sectoral origins of many platforms (Table 2).

Several CRs specify additional domains. SimSpace, for example, does not introduce a new sector but emphasizes that different focus groups are provided with predefined training templates. The iTrust CR maintains a general focus on cyber-exercises, which is noteworthy as CRs can also serve other purposes, such as training in system hardening, hardware and software configuration, or product testing. The Virginia CR targets educators in high schools, community colleges, and universities, forming a specialised subset of academia & research by primarily supporting hands-on student education. Similarly, the Airbus CR, the UNSW CR, BUTCA and the Ohio CR (which covers K-12 education in the U.S.[3]) emphasize a broader "Cyber Education" category.

Further specialisations include RGCE with research & development (R&D) and international collaboration, the Luxembourg CR with humanitarian organisations, Cybexer that targets diverse sectors including finance, smart cities, space systems and managed security service providers (MSSPs), and CDeX with the maritime domain. Fig. 9 provides an overview of the various focus areas and their prevalence among the surveyed CRs.

Regarding accessibility, 30 CRs are open to multiple user groups, while 11 impose access restrictions – six restrict access to academia & research, six to governmental authorities, five to the military, four to critical infrastructure providers, and three to the industry. Eight also specified additional criteria. Of the 29 CRs with declared focus areas (see Section V-C), only five target exclusively a single group and they are all associated with academia & research (see Table 5): SPHERE is focused on the government sector and the other four CRs align with the sector to which their CR itself belongs – academia & research.

Among restricted platforms, the Ohio CR allows access only to Ohio-based non-profit organisations, whereas others may access it for a fee on a project basis. ICE&T requires approval by RI CODE and Cyrange currently limits access to beta testers. Seven of the restricted CRs also define focus groups. KYPO CRP and Laokoon limit access to EU/NATO members. CRATE, which is operated by FOI (Swedish Defence Research Agency) [82] however, restricts access broadly without naming specific target groups.

All 11 CRs with access restrictions are training providers, some (e.g., ICE&T, Cyrange) exclusively so. This is unsurprising, as vendors and Open Source platforms typically do not limit access. Restrictions often correlate with military affiliations or information protection concerns. Of the five CRs restricting access to military users, four are affiliated with that sector. KYPO CRP and Laokoon also cite political alignment as a reason for restrictions. Given the use of CRs in cyber defence and offence training for IT-experts, such limitations are expected in sensitive environments.

[3]https://www.k12academics.com/education-united-states

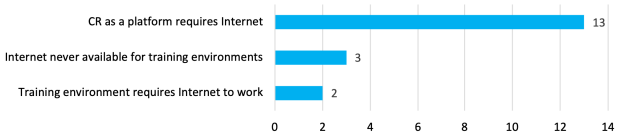


FIGURE 10. Cyber range internet availability on-premise (N = 33).

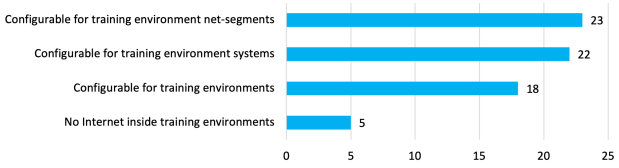


FIGURE 11. Cyber range internet configurability on-premise (N = 33).

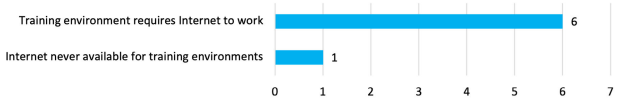


FIGURE 12. Cyber range internet availability cloud (N = 23).

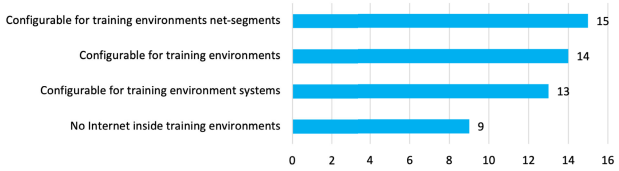


FIGURE 13. Cyber range internet configurability cloud (N = 23).

2) INTERNET REQUIREMENTS AND CONFIGURATION OPTIONS

Our survey also targeted to provide the Internet requirement and configurability options of CRs in a granular picture, both for on-premise and cloud platforms. This is presented in Table 6.

We distinguish between (a) Internet connectivity required for platform operation and (b) Internet availability within training environments. Among 33 on-premise CR platforms, 13 – exclusively training providers – require Internet access to operate the platform. Two of these (Tecnalia CR and SPHERE) also depend on Internet access for the training environment, although this does not necessarily mean trainees have Internet access inside the training environment. In contrast, MCR, RGCE, and CyTrONE entirely prohibit Internet access within training environments (e.g., no web browsing or downloads), as shown in Fig. 10.

Fig. 11 illustrates the granularity with which Internet access can be configured in on-premise CRs. For 18 platforms, settings apply at the environment level, 23 support

TABLE 6. Cyber range internet requirements.

Cyber Range	On-Premise Product					Cloud Product			
	Internet Required		Internet Configurable			Training Internet Required	Internet Configurable		
	Platform	Training	Training Environment	Training Environment Network	Training Environment Systems		Training Environment	Training Environment Network	Training Environment Systems
ICE&T	×	+	✓	✓	✓	–	–	–	–
CySOP	×	+	/	✓	✓	–	–	–	–
Immersive	–	–	–	–	–	+	✓	✓	✓
iTrust Labs	×	+	✓	✓	✓	+	✓	✓	✓
TELECOM Nancy Cyber Range	!	+	✓	✓	✓	–	–	–	–
Vigrid	×	+	✓	✓	✓	–	–	–	–
SPHERE	!	!	/	/	/	–	–	–	–
CENTS + RangeOS	×	+	✓	✓	✓	+	✓	✓	✓
Laokoon Attack XPerience	×	+	✓	✓	✓	+	✓	✓	✓
MCR	!	×	/	/	/	–	–	–	–
KYPO CRP	–	–	–	–	–	+	/	✓	/
Cyber Simulation Center	!	+	✓	✓	✓	–	–	–	–
Cyrange	!	+	/	✓	/	–	–	–	–
EDURange	×	+	/	✓	/	!	/	/	/
Virginia Cyber Range	–	–	–	–	–	+	✓	✓	✓
CRATE	×	+	✓	✓	✓	–	–	–	–
RGCE	×	×	/	/	/	–	–	–	–
BUTCA	–	–	–	–	–	!	/	/	/
OCR	×	+	✓	✓	✓	–	–	–	–
Luxembourg Cyber Range	×	+	/	/	✓	–	–	–	–
PAIDEUSIS	!	+	/	/	✓	–	–	–	–
Tecnalia Cyber Range Laboratory	!	!	/	/	/	–	–	–	–
Airbus CyberRange	×	+	✓	✓	✓	+	✓	✓	✓
M&NTIS Platform	×	+	/	✓	/	+	/	✓	/
CYRIN	×	+	✓	/	✓	+	✓	/	✓
Range365	–	–	–	–	–	+	✓	✓	✓
CyTrONE	!	×	/	/	/	×	/	/	/
Cybermentis	–	–	–	–	–	!	/	/	/
RangeForce Cyber Readiness Platform	–	–	–	–	–	!	/	/	/
Cybels	!	+	✓	✓	✓	–	–	–	–
UNSW Cyber Range	!	+	/	✓	/	+	✓	✓	✓
SimSpace Platform	×	+	✓	✓	✓	+	✓	✓	✓
CRACK	×	+	/	/	✓	–	–	–	–
Mizzou Cyber Range	–	–	–	–	–	!	/	/	/
Ohio Cyber Range	!	+	✓	✓	✓	–	–	–	–
Coliseum	×	+	✓	✓	✓	+	✓	✓	✓
DIATEAM Hybrid Cyber Range	×	+	/	/	✓	–	–	–	–
CybExer Cyber Range	×	+	✓	✓	✓	+	✓	✓	✓
Cyberbit Range	×	+	/	✓	/	!	/	/	/
AIT Cyber Range	!	+	✓	✓	✓	+	✓	✓	✓
CDeX	!	+	✓	✓	/	+	✓	✓	/

! = Internet is always required, × = Internet is never available, + = Internet is configurable, ✓ = possible, / = not possible, – = no such product

configuration by network segment and 22 allow per-system configuration, which is the most detailed option. Five platforms provide no Internet access within the training network at all. In summary, 28 of 33 on-premise CRs allow granular control. Of the five CRs where this is not the case, three have no Internet available at all.

Cloud-based CRs inherently require network connectivity (even for privately hosted instances on internal networks). However, only six of 23 cloud platforms require Internet access within the training environment for full functionality (see Fig. 12).

CyTrONE is the only cloud-based platform where Internet access is entirely disabled within the training environment, including for internal functions, and one of nine platforms where no system within the training environment can access the Internet. Fig. 13 shows that 14 cloud platforms support environment-level configuration, 15 segment-level, and 13 system-level.

In summary, most CRs support granular Internet access control within training environments. This can be crucial when simulating realistic networks, restricting toolsets for didactic purposes, or mitigating risks (e.g., data exfiltration or malware propagation). Another key finding is that many on-premise CRs can operate without Internet connectivity. The 13 platforms which cannot are training providers who require connectivity to deliver their training content. However, the ability to be operationable without an active Internet connection enables a flexible, mobile deployment, even in offline scenarios.

3) MAINTENANCE, SUPPORT, AGREEMENTS, AND ALIGNMENTS

Other features targeted by our survey in the category 'Product Access' are (i) the available support models, (ii) SLAs, (iii) NDAs, and (iv) the regulation / standard alignments of the CR platforms and their providers. This is presented in Table 7.

TABLE 7. Cyber range maintenance, support, agreements, and alignments.

Cyber Range	Support Model								Service Level Agreements			Non Disclosure Agreements	Regulation / Standard Alignments
	Support Quality		Provider		Maintenance			Updates	Different Levels Specified	Tenant-Specific	Exclusions		
	Professional	Best Effort	Platform Provider	3rd Party	Platforms Included	Individual Agreements	Self						
ICE&T	✓	×	✓	×	A	×	×	R, Cr, On-site	N/A	N/A	N/A	✓	GDPR
CySOP	✓	×	✓	×	A	×	✓	R, Cr, OTA	✓	×	SLD, TZD	✓	AS9100D, ISO/IEC: 9001 + 14001 + 17025 + 27001 + 27701 + 45001, UK Cyber Essentials PLUS
Immersive	✓	×	✓	✓	A	×	✓	OTA	×	✓	–	✓	–
iTrust Labs	✓	×	✓	✓	A	×	×	R	×	✓	–	✓	PDPA
TELECOM Nancy Cyber Range	✓	×	✓	✓	A	×	×	R	×	✓	–	✓	N/A
Vigrid	×	✓	✓	×	A	×	✓	OSCR	N/A	N/A	N/A	×	None
SPHERE	–	–	–	–	–	–	–	–	N/A	N/A	N/A	×	N/A
CENTS + RangeOS	✓	×	✓	×	A	×	×	On-Site	×	✓	–	✓	ISO/IEC 27001 + 27017/27018, NIST RMF, GDPR, SOC-2 (Type 2), PCI DSS, CMMC-2 Certification
Laokoon Attack XPerience	✓	×	✓	×	A	×	×	On-Site	×	✓	–	✓	GDPR
MCR	✓	×	×	✓	A	×	×	R, On-Site	N/A	N/A	N/A	✓	None
KYPO CRP	✓	×	✓	×	A, Dp(O)	✓	Dp(O)	R, On-Site, Dp(O), OSCR	×	✓	–	✓	-
Cyber Simulation Center	✓	×	✓	×	A	×	×	On-Site	×	✓	–	✓	GDPR, ISO/IEC 27001
Cyrange	✓	×	✓	×	A	×	×	On-Site	N/A	N/A	N/A	×	–
EDURange	×	✓	✓	×	A	×	✓	–	N/A	N/A	N/A	×	–
Virginia Cyber Range	✓	×	✓	✓	A	×	×	R, Cr, OTA	N/A	N/A	N/A	✓	FERPA, CIPA
CRATE	✓	×	✓	×	A	✓	×	R, Cr, On-Site	✓	×	SLD	×	GDPR
RGCE	✓	×	✓	×	A	×	×	R, Cr, On-Site	N/A	N/A	N/A	✓	GDPR
BUTCA	✓	×	✓	–	A	–	–	Cr, OTA	–	–	–	✓	CZ/EU law incl. GDPR
OCR	✓	×	✓	×	A, Dp(C)	✓	Dp(O)	R, Cr, OSCR	×	✓	Hardware & Infrastructure	✓	N/A
Luxembourg Cyber Range	✓	×	✓	✓	A	×	×	R, On-Site	–	–	–	✓	GDPR
PAIDEUSIS	✓	×	✓	×	A	×	×	R, OTA	×	✓	–	✓	GDPR
Tecnalia Cyber Range Laboratory	✓	×	✓	×	A	×	×	OTA	N/A	N/A	N/A	×	None
Airbus CyberRange	✓	×	✓	×	C, Dp(O)	×	×	R, Cr	✓	×	SLD	✓	defined based on the specific deployment and customer requirements
M&NTIS Platform	✓	×	✓	×	A	×	×	R, Cr, On-Site	N/A	N/A	N/A	✓	GDPR
CYRIN	✓	×	✓	×	C, Dp(O)	✓	Dp(O)	R, Cr, Dp(O)	×	✓	–	✓	GDPR
Range365	✓	×	✓	×	C	×	×	R, Cr, OTA	✓	–	Comparable to cloud providers	✓	NIST best practices
CyTrONE	×	✓	✓	×	A	×	✓	OSCR	N/A	N/A	N/A	×	N/A
Cybermentis	–	–	–	–	–	–	–	–	N/A	N/A	N/A	✓	–
RangeForce Cyber Readiness Platform	✓	×	✓	×	C	×	×	R, Cr, OTA	✓	×	TZD	✓	SOC-2 (Type 2)
Cybels	✓	×	✓	–	A	–	×	–	–	–	–	✓	None
UNSW Cyber Range	✓	×	✓	✓	A	×	×	–	N/A	N/A	N/A	×	Internal courses and their accreditations
SimSpace Platform	✓	×	✓	×	A	×	×	R, OTA, On-Site, Dp(O)	✓	×	Custom training content, 3rd-party & higher power influence, failures because of own hardware or non-best-practice actions	✓	Training Program: NIST 800-171, SOC2; Corporate data center: SSAE18 SOC1 + 2 + 3, PCI DSS, ISO/IEC 27001 + 1400 + 9001
CRACK	×	✓	✓	×	A	×	✓	OSCR	N/A	N/A	N/A	✓	–
Mizzou Cyber Range	×	✓	✓	×	A	×	✓	OTA	N/A	N/A	N/A	×	N/A
Ohio Cyber Range	✓	×	✓	✓	A	×	×	–	✓	×	–	✓	ISO/IEC 21001 + 27001, FERPA, NIST 800-171
Coliseum	✓	×	✓	×	A	✓	Dp(A)	–	×	✓	–	✓	Defined based on the specific deployment and customer requirements
DIATEAM Hybrid Cyber Range	✓	×	✓	–	A	–	×	OTA, Dp(O)	N/A	N/A	N/A	✓	–
CybExer Cyber Range	✓	×	✓	✓	A	✓	×	Dp(A), R, Cr, OTA, On-Site	✓	✓	SLD, TZD	✓	GDPR, ISO/IEC 27001
Cyberbit Range	✓	×	✓	×	C, Dp(O)	✓	Dp(O)	Cr, OTA, On-Site, Dp(O)	–	✓	–	✓	GDPR, ISO/IEC 27001, 3rd party pentest
AIT Cyber Range	✓	×	✓	×	A	×	×	R, Cr	×	✓	–	✓	ISO certified, GDPR, Austrian law
CDeX	✓	×	✓	×	A	×	Dp(O)	OTA, On-Site, Dp(O)	✓	✓	SLD	✓	None

✓ = Yes, × = No, – = No information provided, N/A = Not available, A = For all products, C = For cloud products, O = For on-premise products, Dp() = Product type in brackets depends on individual agreement, R = Regular updates, Cr = Critical updates, OTA = Over the air updates, On-Site = On-Site updates, OSCR = Updates via Open Source Code Repository, SLD = Depends on Service Level, TZD = Depends on timezone

As the corresponding questions were mostly answered as free text, the detailed answers can be found in the published survey results[4] or by using our CR search engine.[5]

SLAs are supported by 25 CRs, while 16 do not offer them. Of the 25 CRs, 22 provided detailed information: Nine offer predefined SLAs with multiple service levels, 15 define them individually or on request. CDeX and CybExer support both models. SimSpace[6] and Keysight

[4]https://doi.org/10.60776/F1WOHD

[5]https://go.unibw.de/cyber-range-comparison

[6]https://simspace.com/service-level-agreement/

with CySOP,[7] however, linked their SLAs online. The CR providers that offer predefined SLAs also named exclusions from their SLAs more frequently, typically related to service levels or support hours. However, OCR is an exception here: only individual SLAs are offered, but hardware and infrastructure are excluded. This means, SLAs can only be negotiated for the software.

NDAs are supported by 32 CRs, and 23 align with established regulations or standards. These are mostly national or regional data protection regulations like the GDPR (13x) [18] or security certifications for data centres like ISO/IEC 27001 (7x). Noteworthy, all 23 that adhere to regulations or standards are training providers, with 15 belonging to the industry sector. Additionally, 21 of them offer training via web or VPN, further reinforcing the insight that CRs which provide remote access are more likely to comply with formal regulatory frameworks. SLA support, however, is also more common in the industry sector (17 of 18 CRs), with Cybermentis as the only exception. Among the 38 training providers, 24 support SLAs. Notably, of the 14 that do not, 11 are associated with academia & research. This suggests SLAs are more prevalent in industry settings where availability guarantees are expected. Notably, ICE&T and Cyrange – which are the two on-site only CRs – do not offer SLAs, while also 12 of 36 remote-access CRs lack them. In contrast, NDAs are even more widespread and standard in commercial CRs. All nine CRs without NDA support belong to academia & research.

Professional support is offered by 34 of 39 CRs. Exceptions originate exclusively from Open Source or academia, where support is typically offered on a best-effort basis. The support offering is provider-managed in 38 cases, with MCR as the sole exception. Nine CRs also allow third-party support. These CRs are all remote training providers, with third-party support primarily covering aspects unrelated to the CR software itself, such as hardware support.

Across all CRs, support is consistently available for all deployment types. However, some platforms limit standard support to cloud versions, with on-premise support requiring individual agreements (e.g., Airbus CR, CYRIN, or Cyberbit Range). KYPO's cloud version includes professional support, whereas its Open Source version is best-effort unless contracted separately.

Self-managed maintenance is required by seven CRs. Additionally, six more may require self-maintenance depending on the individual agreement. Notably, six of 13 CRs requiring user-managed maintenance are from the industry sector, showing that this is not limited to Open Source or academic platforms.

Regarding updates (see Fig. 14), 34 CRs provided input. The survey question was open-ended here. However, regular updates are standard: 20 mentioned general updates, 15 critical updates, 15 on-site updates, and 12 over-the-air (OTA) updates. The update strategy (OTA vs on-site) can be an important factor for organisations considering the acquisition or use of a CR, particularly if they must comply with specific security policies or restrictions.

[7]https://www.keysight.com/us/en/assets/7019-0298/brochures/Global-Test-Solutions-Support.pdf

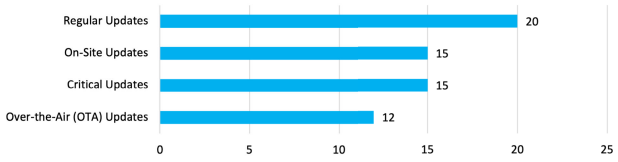


FIGURE 14. Cyber range update model (N = 34).

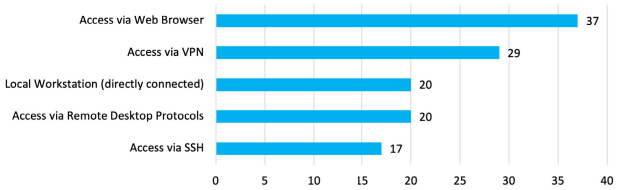


FIGURE 15. Cyber range trainee access method (N = 41).

D. RESULTS REGARDING PLATFORM ACCESS

In the following, the results for the accessibility category 'Platform Access' are outlined. This contains platform access and training scenario availability limitations, but also the technical connection methods for trainees to connect into their CR training.

1) PLATFORM AND SCENARIO AVAILABILITY

Table 8 summarises restrictions on CR platform access, like user licensing or the parallel use of training environments and scenarios. Regarding platform availability, 33 CRs reported no limitations, whereas eight cited specific restrictions – mostly tied to office hours (e.g., ICE&T, AIT, iTrust Labs on-site) or instructor availability (EDURange). RGCE allows access based on prior agreement, and Immersive dynamically restricts access depending on system load.

For user licensing, parallel environments, and training scenarios, data is available from 40 CRs, excluding SPHERE. User licensing is unrestricted in 27 CRs. However, 13 reported constraints. Four CRs cited technical limitations such as hardware, VPN capacity, or licensing. The remaining nine CRs imposed user licensing restrictions. Some enforce fixed maximum capacities for concurrent users. In contrast, CySOP, the Coliseum, and the Cyberbit cloud-offering adopt flexible licensing models without predefined user caps.

With regard to parallel training environments, 28 CRs impose no limits. Eight cite infrastructure related restrictions (e.g., hardware or virtualisation licences). The other four CRs limit usage based on the number of licences available: ICE&T allows eight environments, CySOP supports up to 120, depending on licence, and M&NTIS and Cyberbit (cloud) base limits on training plans/bookings.

TABLE 8. Cyber range platform access limitations.

Cyber Range	Platform Availability	User Licensing	Parallel Training Environments	Parallel Training Scenarios
ICE&T	Limited by office hours	At maximum, 64 users at a time	At maximum 8 per scenario	At maximum 2
CySOP	×	Licensing bundles, starting from 10 users; then incremental packages in steps of 5	Depending on bundles purchased; up to 120 simultaneous tenants	Depending on bundles purchased; up to 120 simultaneous tenants
Immersive	Limited by running CPU/RAM levels	×	Limited by CPU/RAM purchased	Limited by CPU/RAM purchased
iTrust Labs	On-site use limited by office hours	Depends on use of on-site testbed vs. digital twins	Depends on use of on-site testbed vs. digital twins	Depends on exercise design
TELECOM Nancy Cyber Range	×	×	×	×
Vigrid	×	Depends on hardware deployed	Depends on hardware deployed	Depends on hardware deployed
SPHERE	×	N/A	N/A	N/A
CENTS + RangeOS	×	×	×	×
Laokoon Attack XPerience	×	×	×	×
MCR	×	At maximum 20 users at a time	×	At maximum one per training session
KYPO CRP	×	×	×	×
Cyber Simulation Center	×	×	×	×
Cyrange	×	Limited by VirtualBox licence	Limited by VirtualBox license	Limited by VirtualBox license
EDURange	Limited by instructor availability	×	×	×
Virginia Cyber Range	Limited by support office hours	At maximum 500 users in one class	×	×
CRATE	Limited by support office hours	×	×	×
RGCE	Limited by individual agreed access timeframes	×	×	×
BUTCA	×	User licences required	Based on licensed seats	Limited by license and number of seats
OCR	×	×	×	×
Luxembourg Cyber Range	×	Limited by number of simultaneous VPN connections and underlying hardware	×	×
PAIDEUSIS	×	×	Limited by underlying hardware	Limited by underlying hardware
Tecnalia Cyber Range Laboratory	×	At maximum 20 users in on-site training	×	×
Airbus CyberRange	×	×	×	×
M&NTIS Platform	×	×	Depends on the purchased training plan	Depends on the purchased training plan
CYRIN	×	×	×	On-premise: Depends on hardware deployed
Range365	×	10 to 50 blue team workstations depending on licensing	×	At maximum one per training session
CyTrONE	×	×	×	×
Cybermentis	×	×	×	×
RangeForce Cyber Readiness Platform	×	×	×	×
Cybels	×	×	×	×
UNSW Cyber Range	×	×	×	×
SimSpace Platform	×	×	Depends on hardware deployed	Depends on hardware deployed
CRACK	×	×	×	×
Mizzou Cyber Range	×	×	×	×
Ohio Cyber Range	×	×	×	×
Coliseum	×	Variable licensing	Depends on hardware deployed	×
DIATEAM Hybrid Cyber Range	×	×	×	×
CybExer Cyber Range	×	×	×	×
Cyberbit Range	×	On-premise: maximum 12 users per class; Cloud: licensed by users per year	On-premise: Depends on hardware deployed; Cloud: Multiple parallel bookings supported	On-premise: Depends on hardware deployed; Cloud: Limited by number of exercises bought
AIT Cyber Range	Limited by office hours	×	×	×
CDeX	×	×	×	×

× = no such limitation, N/A = no information provided

Regarding parallel training scenarios, 26 CRs reported no restrictions. Again, seven cite technical constraints. MCR and Range365 allow one scenario per session, while ICE&T allows two. CySOP mirrors its environment policy (up to 120). The rest bases limits on licence terms or user quotas.

Across categories, platform availability limitations are less frequent (8 CRs) than licensing-related or technical constraints on users (13), environments (12), or scenarios (14). Notably, all CRs with platform availability restrictions are provider-managed during training. Immersive is the only CR to explicitly cite hardware capabilities as the reason for this. However, similar constraints likely apply elsewhere under full system load.

Technical factors are more often the root cause of restrictions than licensing. While only Immersive cited technical limitations in terms of platform accessibility, four CRs named those for user access, eight for parallel training environments, and seven for parallel training scenarios. This suggests that hardware capacity is a more common bottleneck than the licensing policy.

In summary, while some CRs face access limitations – mostly due to hardware or operational constraints – the majority does nevertheless offer sufficient flexibility to meet diverse organisational training needs. Overall, most CRs do not impose restrictions on platform accessibility, supported users or simultaneous execution of training scenarios and environments.

2) TRAINEE PLATFORM ACCESS

Table 9 and Fig. 15 present how trainees access their training environments. This concerns the methods that are available to access a training environment (e.g., on-site in a training centre) and does not mean how the CR is made accessible as a product, as shown in Table 4.

TABLE 9. Cyber range trainee platform access.

Cyber Range	Local Workstation	VPN	Web Browser	Remote Desktop	SSH
ICE&T	×	✓	×	✓	✓
CySOP	✓	✓	✓	✓	✓
Immersive	×	✓	✓	✓	✓
iTrust Labs	✓	✓	✓	✓	✓
TELECOM Nancy Cyber Range	✓	✓	✓	×	×
Vigrid	✓	✓	×	✓	✓
SPHERE	×	✓	✓	×	×
CENTS + RangeOS	✓	✓	✓	✓	×
Laokoon Attack XPerience	×	✓	✓	✓	✓
MCR	✓	✓	✓	×	×
KYPO CRP	×	✓	✓	×	×
Cyber Simulation Center	×	✓	×	✓	×
Cyrange	✓	✓	✓	✓	✓
EDURange	×	×	✓	×	✓
Virginia Cyber Range	×	×	✓	×	×
CRATE	✓	✓	✓	✓	×
RGCE	✓	✓	✓	✓	×
BUTCA	✓	✓	✓	✓	✓
OCR	✓	✓	✓	✓	✓
Luxembourg Cyber Range	×	✓	✓	✓	✓
PAIDEUSIS	×	✓	✓	×	×
Tecnalia Cyber Range Laboratory	✓	✓	✓	✓	×
Airbus CyberRange	✓	✓	✓	×	×
M&NTIS Platform	×	✓	✓	✓	✓
CYRIN	×	×	✓	×	×
Range365	×	×	✓	×	×
CyTrONE	×	✓	✓	✓	✓
Cybermentis	×	×	✓	×	×
RangeForce Cyber Readiness Platform	×	×	✓	×	×
Cybels	✓	×	✓	×	×
UNSW Cyber Range	✓	×	✓	×	✓
SimSpace Platform	×	×	✓	×	×
CRACK	×	✓	✓	×	×
Mizzou Cyber Range	×	×	✓	×	×
Ohio Cyber Range	×	×	✓	×	×
Coliseum	✓	✓	✓	✓	✓
DIATEAM Hybrid Cyber Range	✓	✓	×	×	✓
CybExer Cyber Range	✓	✓	✓	✓	✓
Cyberbit Range	✓	✓	✓	×	×
AIT Cyber Range	×	×	✓	×	×
CDeX	✓	✓	✓	✓	×

✓ = method available × = method not available

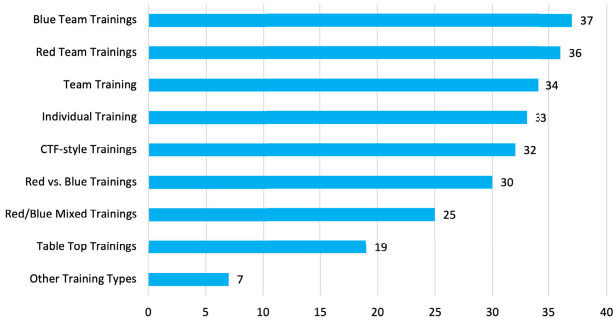


FIGURE 16. Cyber range training types (N = 41).

Most CRs support multiple access methods, with 37 of 41 allowing web browser access, making it the predominant approach (see Fig. 15). VPN access follows with support by 29 CRs. Nine CRs exclusively rely on web access, all of

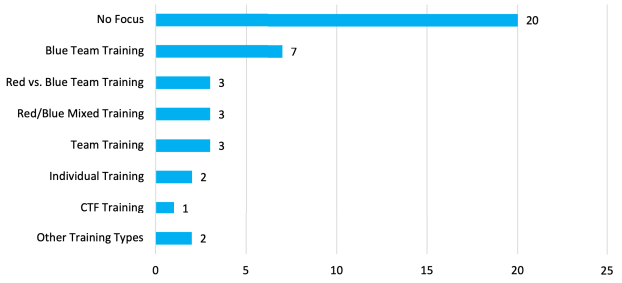


FIGURE 17. Cyber range training types focus (N = 41).

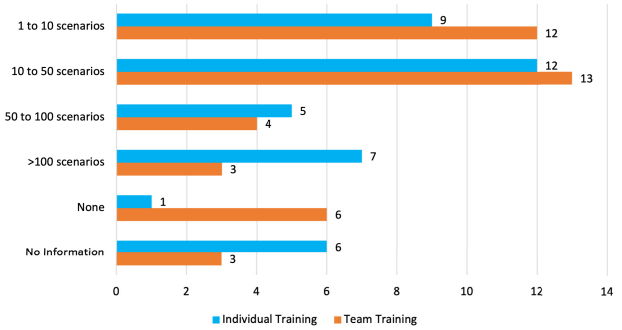


FIGURE 18. Cyber range preconfigured training scenarios (N = 32).

which are web-based training providers (compare Table 4). In contrast, CySOP, iTrust, Cyrange, BUTCA, and the Open CR support all available connection methods.

Four CRs – ICE&T, Vigrid, the Cyber Simulation Center, and the DIATEAM Hybrid CR – do not offer browser-based access. For ICE&T and the Cyber Simulation Center, this aligns with their respective operational models. Vigrid, as a self-hostable Open Source product, operates without a web interface. DIATEAM provides remote training via VPN and in-person access at its training centre but no browser-based option.

E. RESULTS REGARDING TRAINING CONTENT

For the accessibility category 'Training Content', we queried different subtopics: (i) training types and focus, (ii) preconfigured training scenarios and training acknowledgment, (iii) customisation options for the preconfigured training scenarios, (iv) the categories of the preconfigured training scenarios, (v) supported training groups, (vi) attack implementation in training scenarios, and (vii) available simulation features.

1) TRAINING TYPES AND FOCUS

Table 10 summarises the available training types and focuses across CRs, revealing broad support for a diverse set of training formats. Among the 41 CRs, 36 support red team training, 37 blue team training, 30 red vs. blue, and 25 red/blue mixed training. Additionally, 32 offer CTF-style formats, 33 provide individual training, 34 team-based training, and 19 include table-top exercises. Seven CRs report

TABLE 10. Cyber range training type and focus.

Cyber Range	Training Types								Training Focus	Supplementary Information
	Red	Blue	Red vs. Blue	Red/Blue Mixed	CTF	Individual	Team	Table-Top		
ICE&T	✓	✓	✓	✓	×	✓	✓	×	Team	–
CySOP	✓	✓	×	✓	✓	✓	✓	×	×	–
Immersive	✓	✓	×	×	×	×	✓	×	Team	–
iTrust Labs	✓	✓	✓	✓	✓	✓	✓	✓	Red/Blue Mixed	Also offered: C–suite as well as Operator Training, Academic training and Teaching: Trainings refer to CISS and CIDEX
TELECOM Nancy Cyber Range	✓	✓	✓	×	✓	✓	✓	✓	×	–
Vigrid	✓	✓	✓	✓	✓	✓	✓	×	×	The Open Source nature of the product allows to implement own training types
SPHERE	✓	✓	✓	✓	✓	✓	✓	✓	Red vs. Blue	–
CENTS + RangeOS	✓	✓	✓	✓	✓	✓	✓	✓	Red/Blue Mixed	–
Laokoon Attack XPerience	✓	✓	✓	✓	×	✓	✓	✓	Red/Blue Mixed	–
MCR	✓	✓	✓	×	✓	✓	✓	✓	Team	–
KYPO CRP	✓	✓	✓	✓	✓	✓	✓	×	Blue	–
Cyber Simulation Center	×	✓	×	×	×	✓	✓	×	Individual Blue Team Training	–
Cyrange	✓	✓	×	×	×	×	×	×	×	–
EDURange	✓	×	×	×	✓	✓	✓	×	×	–
Virginia Cyber Range	✓	✓	×	×	✓	✓	×	×	Individual	–
CRATE	✓	✓	✓	×	✓	✓	✓	✓	Blue	–
RGCE	✓	✓	✓	✓	✓	✓	✓	✓	×	Also offered: Business Sector Exercises, National Exercises, Purely Technical Hands On Training
BUTCA	✓	✓	✓	✓	✓	✓	✓	✓	×	–
OCR	✓	✓	✓	✓	✓	✓	✓	✓	×	–
Luxembourg Cyber Range	✓	✓	✓	✓	✓	✓	✓	✓	×	–
PAIDEUSIS	×	×	×	×	✓	✓	×	×	CTF	–
Tecnalia Cyber Range Laboratory	✓	✓	×	×	✓	×	×	×	×	–
Airbus CyberRange	✓	✓	✓	✓	✓	✓	✓	✓	×	Also offered: Validation & Testing and Cyberskill assessment
M&NTIS Platform	×	✓	×	×	×	×	✓	×	Blue	–
CYRIN	✓	✓	✓	✓	✓	✓	✓	×	Individual	–
Range365	✓	✓	✓	✓	×	×	✓	×	Blue	–
CyTrONE	✓	✓	✓	✓	✓	✓	✓	×	×	–
Cybermentis	✓	✓	×	✓	×	✓	×	×	Blue	–
RangeForce Cyber Readiness Platform	✓	✓	✓	✓	✓	✓	✓	×	Blue	–
Cybels	✓	✓	✓	×	✓	×	×	×	×	Also offered: Operationol Technology Training
UNSW Cyber Range	✓	✓	✓	×	✓	✓	✓	✓	×	–
SimSpace Platform	✓	✓	✓	✓	✓	✓	✓	✓	Elite Cyber Defense Training	Also offered: Elite Cyber Defense Training; This includes blue and red teaming skills training
CRACK	×	×	✓	×	✓	×	×	×	Red vs. Blue	–
Mizzou Cyber Range	×	×	×	×	×	✓	✓	×	×	–
Ohio Cyber Range	✓	✓	✓	✓	✓	×	✓	✓	×	–
Coliseum	✓	✓	✓	✓	✓	✓	✓	✓	×	Also offered: Mission Rehearsal, Environment Integration and Systems Testing
DIATEAM Hybrid Cyber Range	✓	✓	✓	✓	✓	✓	✓	×	Red vs. Blue	–
CybExer Cyber Range	✓	✓	✓	✓	✓	✓	✓	✓	×	Also offered: Digital Twinning, AI & Technology Testing, Framework Based Skills Testing
Cyberbit Range	✓	✓	✓	×	✓	✓	✓	×	Blue	Red, Blue, CTF, Red vs. Blue supported on-premise; Red/Blue mixed only in Cloud
AIT Cyber Range	✓	✓	✓	✓	✓	✓	✓	✓	×	–
CDeX	✓	✓	✓	✓	✓	✓	✓	✓	×	–

✓ = Training type offered, × = Training type not offered, – = no supplementary information

further training types, but these are provider-specific and no common categories could be identified across multiple providers. Details are available in the "Supplementary Information" column of Table 10.

Notably, all CRs offer multiple training formats, and 13 support all listed types. The table also highlights differences in Cyberbit's cloud and on-premise versions: the former includes red/blue mixed training, while the latter supports red, blue, red vs. blue, and CTF training.

Fig. 16 visualises the distribution of training types. Over 75% of CRs support the major formats, especially blue team (37) and red team (36) training. Red/blue mixed and table-top training are less common, supported by only 25 and 19 CRs, respectively. The limited adoption of table-top exercises likely reflects their non-technical nature and differing requirements.

Regarding training focus, Fig. 17 shows that 20 CRs report no particular focus. Among those that do, the most frequent focus is on defensive training (nine CRs), including the seven prioritising blue team training, as well as the Cyber Simulation Center and SimSpace, which emphasise "Individual Blue Team Training" and "Elite Cyber Defense Training". ICE&T, Immersive, and MCR highlight team dynamics, rather than exclusively offensive or defensive workflows, while the Virginia CR and CYRIN focus on individual skill development.

TABLE 11. Cyber range preconfigured training scenarios availability and acknowledgement.

Cyber Range	Quantity		Form of Availability		Training Acknowledgement
	Individual Training	Team Training	Acquisition	Supplementary Information	
ICE&T	50 to 100	10 to 50	Training offering	–	×
CySOP	50 to 100	×	Included in purchase	–	×
Immersive	N/A	50 to 100	Included in purchase, Extra purchase, Training offering	–	×
iTrust Labs	>100	>100	Extra purchase , Training offering	–	Accountable for the Singapore University of Technology and Design's (SUTD) Master of Science Security by Design (MSSD) program and SUTD Academy
TELECOM Nancy Cyber Range	×	×	Extra purchase , Community developed	–	×
Vigrid	N/A	N/A	×	–	×
SPHERE	>100	50 to 100	Included in purchase	–	×
CENTS + RangeOS	1 to 10	1 to 10	Included in purchase, Extra purchase	Base courses included	Official certification preparation courses: CompTIA, ISC2, EC-Council, Continuing education credits (CEUs) to maintain certifications
Laokoon Attack XPerience	10 to 50	1 to 10	Included in purchase, Training offering	–	×
MCR	10 to 50	10 to 50	Included in purchase, Extra purchase	–	×
KYPO CRP	1 to 10	×	Included in purchase, Extra purchase, Community developed & included	–	×
Cyber Simulation Center	10 to 50	10 to 50	Training offering	–	×
Cyrange	N/A	N/A	×	–	×
EDURange	10 to 50	10 to 50	Community developed & included, Training offering	–	×
Virginia Cyber Range	10 to 50	1 to 10	Included in purchase	–	×
CRATE	1 to 10	1 to 10	Extra purchase, Training offering	–	×
RGCE	>100	>100	Included in purchase, Extra purchase, Training offering	–	×
BUTCA	10 to 50	10 to 50	Included in purchase, Extra purchase, Community developed & included, Training offering	–	×
OCR	10 to 50	1 to 10	Extra purchase, Community developed, Training offering	–	×
Luxembourg Cyber Range	1 to 10	1 to 10	Included in purchase, Extra purchase	–	×
PAIDEUSIS	50 to 100	×	×	–	×
Tecnalia Cyber Range Laboratory	1 to 10	1 to 10	Training offering	–	×
Airbus CyberRange	10 to 50	10 to 50	Included in purchase, Extra purchase, Community developed & included, Training offering	–	×
M&ENTIS Platform	N/A	10 to 50	Included in purchase	–	×
CYRIN	50 to 100	1 to 10	Included in purchase, Training offering	–	CYRIN custom certification which can include (i) digital badges, (ii) Continuing Professional Education credits (CPEs), (iii) Printable certification, and (iv) badge icon s
Range365	N/A	10 to 50	Included in purchase, Training offering	–	Trainees receive custom scenario completion certificates, Cyber Range administrators and trainers are certified by Cloud Range and receive badges in the Cloud Range Performance Portal Learning Management System
CyTrONE	1 to 10	×	Included in purchase, Community developed	–	×
Cybermentis	50 to 100	×	Included in purchase, Training offering	–	×
RangeForce Cyber Readiness Platform	>100	10 to 50	Included in purchase, Training offering	–	Custom Badges and ongoing personal professional training
Cybels	1 to 10	1 to 10	Extra purchase, Training offering	–	×
UNSW Cyber Range	N/A	N/A	×	–	×
SimSpace Platform	>100	10 to 50	Included in purchase, Training offering	–	Credly approved and publically observable certifications and awards
CRACK	1 to 10	1 to 10	Training offering	–	×
Mizzou Cyber Range	1 to 10	1 to 10	Community developed	–	×
Ohio Cyber Range	×	50 to 100	Community developed, Training offering	–	Continuing Education Crredits (CEUs) for Ohio Cyber Guardian annual red vs. blue training, Anally K-12 teaching education programs, Bootcamp completion certifications for industry recognised credential aligned bootcamps, Cyber Mindfulness and Local Government Entity training badges provided for Ohio Persistent Cyber Improvement project
Coliseum	10 to 50	10 to 50	Extra purchase	–	×
DIATEAM Hybrid Cyber Range	10 to 50	1 to 10	Extra purchase	–	×
CybExer Cyber Range	10 to 50	10 to 50	Included in purchase, Extra purchase, Training offering	Scenario sharing via federated Cybexer Ranges possible; community development possible, but not used yet	Trainings generally aligned with NIST NICE framework, Trainings and exercises individually aligned to multiple government customers with their national or organisational bodies' certification programs (e.g., within army accepted certificates)
Cyberbit Range	>100	50 to 100	Included in purchase, Training offering	–	ISC2: Every hour spent on training is valid 1 CPE credit, Preparation courses for COMPTIA Certification: Security+, Network+, CySA+
AIT Cyber Range	10 to 50	10 to 50	Included in purchase, Training offering	–	Training are defined and confirmed in accordance with European or national regulations
CDeX	>100	>100	Included in purchase, Extra purchase	–	×

× = Not available, N/A = No information provided, – = No supplementary information

While many CRs do not prioritise a single type, those that do tend to focus on defensive or team-oriented training strategies. However, no distinct overall orientation of CRs can be inferred from the numbers presented in Fig. 17.

2) PRECONFIGURED TRAINING SCENARIOS

Table 11 summarises the quantity and accessibility of preconfigured training scenarios and indicates whether they are awarded with certifications that are officially recognised in the industry. Among 41 CRs, 35 provide individual training

scenarios: nine offer 1-10, 12 offer 10-50, five offer 50-100, and seven offer more than 100. Six CRs did not specify a number, including the Ohio CR and the TELECOM Nancy CR, which explicitly do not offer such scenarios.

For team training, 32 CRs provide scenarios in similar quantities: 12 provide 1-10, 13 offer 10-50, four provide 50-100, and three offer more than 100 scenarios. Nine CRs have no team training scenarios, including Vigrid, Cyrange, and the UNSW CR, which lack preconfigured content entirely.

As Fig. 18 visualises, most CRs offer both individual and team scenarios, typically within the 1-50 range. This includes the Open Source platforms with Vigrid as the only exception.

In 23 CRs, the scenarios are already included with the platform at no extra cost. Another 23 make them available when booking a training session. Nine provide free, community-developed content and 17 offer additional scenarios for purchase. Platforms like KYPO CRP, EDURange, BUTCA, and the Airbus CR include such community content by default, while CybExer enables scenario sharing between federated Cybexer CRs. PAIDEUSIS, though reporting 50-100 individual training scenarios, did not clarify access conditions. However, scenario availability is likely tied to booked trainings, given its web/VPN-only access model.

Only 11 of 41 CRs provide training programs with formal acknowledgment or accreditation. Most of these are found among commercial providers. Exceptions include iTrust, which offers accredited courses for the Singapore University of Technology and Design (SUTD), and the Ohio Cyber Range, which provides widely recognised accreditation, including Continuing Education Credits (CEUs), K-12 teaching education programs, and training badges meeting the requirements of local government entities. However, officially recognised CR training is not the industry standard.

CEUs and CPEs are the most common accreditation forms. Both are credits that are commonly awarded for acknowledgement in the cybersecurity field. CEUs equate to 10 contact hours, CPEs to 50 minutes of instruction by a qualified professional [91]. While some platforms (e.g., CyberCENTS and Cyberbit) offer fully accredited CEU/CPE-compatible programs, others provide custom certifications. For example, SimSpace uses Credly-approved but customised certifications. However, Credly provides a platform for issuing and managing digital credentials, which is widely used by organisations to verify professional achievements [92].

Some CRs align with established regulatory frameworks rather than formal accreditation. CybExer structures its training according to the NIST NICE framework and government client needs. Similarly, the AIT designs its programs to meet EU/national regulations. These approaches demonstrate that while formal certification is rare, regulatory alignment offers an alternative path to offer officially acknowledged training.

3) PRECONFIGURED TRAINING SCENARIO CUSTOMIZATION

For examining the adaptability of preconfigured training scenarios, it must be assessed whether modifications to the network topology, included systems, and cyberattacks within a scenario are possible. This level of customisability is especially relevant when adapting training scenarios to specific customer requirements. Therefore, we queried whether CRs allow modifications to their scenarios' network topology, systems, and cyberattacks. Additionally, we asked whether CRs allow the development of custom training scenarios beyond preconfigured options and who is able to do so. The corresponding data is presented in Table 12.

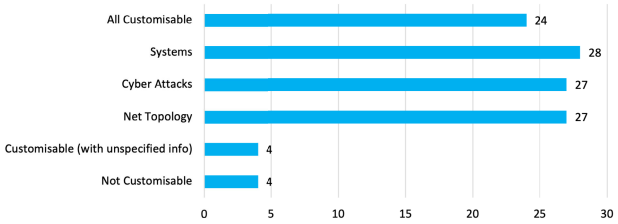


FIGURE 19. Cyber range customisation (N = 38).

Cyrange, Vigrid, and the UNSW CR do not offer preconfigured scenarios (see Table 11), and thus no customisation is possible. Four other CRs (PAIDEUSIS, the Tecnalia CR Lab, Cybermentis, and the Mizzou CR) explicitly stated that their training scenarios cannot be customised. The remaining 34 CRs allow scenario customisation and 30 of these provided detailed information on their scenario modification options.

Among these 30 CRs, 24 allow full customisation of topology, systems, and cyberattacks. In the remaining cases, customisation is partially restricted: CySOP, the TELECOM Nancy CR, and the Virginia CR do not support attack modification. Range365 and RangeForce do not allow changes to systems or topology. M&ENTIS, however, does not permit network topology adjustments. Fig. 19 highlights these results.

Custom training scenarios can generally be created on all 41 CR platforms. In 40 cases, the provider can do so. EDURange is the only exception here. Customers can create and customise their own scenarios on 28 platforms. The remaining CRs restrict this option, typically because they focus on delivering training services.

However, if a scenario is to be tailored specifically to an industry, a cyber threat, or a customer and its network infrastructure, it must be possible to develop such a scenario from scratch. Technically very experienced customers can operate their own CR and develop scenarios customised to their demands there. Otherwise, customers are more likely to order training scenarios from the CR operators and support them in customising these scenarios to their needs.

4) PRECONFIGURED TRAINING SCENARIO CATEGORIES

In addition to the customisability of training scenarios, the survey examined the training categories covered by preconfigured scenarios. Data from the 38 CRs offering

TABLE 12. Cyber range preconfigured training scenario customisation.

Cyber Range	Preconfigured Scenario Customisation					Custom Scenario Creation	
	Overall	Net Topology	Systems	Attacks	Supplementary Information	By Customer	By Provider
ICE&T	✓	✓	✓	✓	–	×	✓
CySOP	✓	✓	✓	×	–	✓	✓
Immersive	✓	✓	✓	✓	–	✓	✓
iTrust Labs	✓	–	–	–	–	✓	✓
TELECOM Nancy Cyber Range	✓	✓	✓	×	–	✓	✓
Vigrid	N/A	N/A	N/A	N/A	–	✓	✓
SPHERE	✓	–	–	–	–	×	✓
CENTS + RangeOS	✓	✓	✓	✓	–	✓	✓
Laokoon Attack XPerience	✓	✓	✓	✓	–	×	✓
MCR	✓	✓	✓	✓	Customizable traffic flows	✓	✓
KYPO CRP	✓	–	–	–	–	✓	✓
Cyber Simulation Center	✓	✓	✓	✓	–	×	✓
Cyrange	N/A	N/A	N/A	N/A	–	✓	✓
EDURange	✓	✓	✓	✓	–	✓	×
Virginia Cyber Range	✓	✓	✓	×	–	×	✓
CRATE	✓	✓	✓	✓	Automatic scenario randomizer available	✓	✓
RGCE	✓	✓	✓	✓	–	✓	✓
BUTCA	✓	✓	✓	✓	–	✓	✓
OCR	✓	✓	✓	✓	–	✓	✓
Luxembourg Cyber Range	✓	✓	✓	✓	–	✓	✓
PAIDEUSIS	×	×	×	×	–	×	✓
Tecnalia Cyber Range Laboratory	×	×	×	×	–	×	✓
Airbus CyberRange	✓	✓	✓	✓	–	✓	✓
M&NTIS Platform	✓	×	✓	✓	Attacks customisable by setting execution time or pausing/resuming at specific steps	×	✓
CYRIN	✓	✓	✓	✓	Licence for CYRIN's Exercise Builder tool required	✓	✓
Range365	✓	×	×	✓	–	✓	✓
CyTrONE	✓	✓	✓	✓	–	✓	✓
Cybermentis	×	×	×	×	–	×	✓
RangeForce Cyber Readiness Platform	✓	×	×	✓	–	×	✓
Cybels	✓	–	–	–	Implementing customisation requests depends on estimated workload	✓	✓
UNSW Cyber Range	N/A	N/A	N/A	N/A	–	✓	✓
SimSpace Platform	✓	✓	✓	✓	–	✓	✓
CRACK	✓	✓	✓	✓	Systems and services available from a predefined catalogue; scoring adjustments possible	×	✓
Mizzou Cyber Range	×	×	×	×	–	×	✓
Ohio Cyber Range	✓	✓	✓	✓	–	✓	✓
Coliseum	✓	✓	✓	✓	–	✓	✓
DIATEAM Hybrid Cyber Range	✓	✓	✓	✓	–	✓	✓
CybExer Cyber Range	✓	✓	✓	✓	–	✓	✓
Cyberbit Range	✓	✓	✓	✓	Only on-premise supports full customisation; Cloud version allows only customisation of selectable security tools	✓	✓
AIT Cyber Range	✓	✓	✓	✓	–	×	✓
CDeX	✓	✓	✓	✓	–	✓	✓

✓ = Possible, × = Not possible, N/A = no information provided, – = No supplementary information

such scenarios is presented in Table 13. However, certain categories require a definition to precisely grasp their scope:

- *Incident Response (IR)*: Training for analysing logs, artifacts, and other evidence to determine cause, scope, and impact of a security incident. IR follows a reactive cybersecurity approach, which means it deals with cyberattacks after these have already occurred.
- *Security Operations Centre (SOC) Teaming*: This training involves monitoring identities, endpoints, servers, databases, network applications, websites, and other systems to detect potential cyberattacks in real-time. The scope of SOC operations extends beyond mere threat detection – it also includes threat analysis, investigation of attack sources, vulnerability reporting, and implementing security improvements. A SOC team, therefore, operates in real-time response while simultaneously working on optimising an organisation's overall security posture.
- *Threat Hunting*: Unlike a SOC, threat hunting takes a proactive approach. It involves analysing logs, network traffic, endpoint data, and other relevant security information to detect hidden or advanced threats before they cause damage. Threat hunters actively search for malicious activities within an organisation's network, aiming to identify and mitigate cyber threats at an early stage.
- *Forensics*: This category involves systematic analysis of storage and network data to investigate incidents. Forensic training focuses on securely extracting and analysing system data (e.g., system images) in compliance with legal standards, making the findings admissible in court. Unlike IR, forensics training is not centred on

TABLE 13. Available training scenario categories.

Cyber Range	IR	SOC	Threat Hunting	Forensics	CRITIS / OT	IoT	Mobile	Network Analysis	Malware Analysis	Linux Analysis	Windows Analysis	MacOS Analysis	Pen-Testing	Malware Devel-opment	Further Scenario Categories
ICE&T	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	✓	×	–
CySOP	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	✓	×	–
Immersive	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	✓	×	–
iTrust Labs	✓	✓	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	OT training
TELECOM Nancy Cyber Range	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	–
Vigrid	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SPHERE	✓	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	–
CENTS + RangeOS	✓	×	✓	×	✓	×	×	✓	✓	×	×	×	✓	✓	–
Laokoon Attack XPerience	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	–
MCR	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	–
KYPO CRP	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	–
Cyber Simulation Center	✓	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	×	×	–
Cyrange	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
EDURange	×	×	×	×	×	×	×	✓	✓	✓	×	×	✓	×	Web App
Virginia Cyber Range	✓	×	×	✓	×	×	×	✓	×	✓	✓	×	✓	×	–
CRATE	✓	✓	✓	×	✓	×	×	✓	×	✓	✓	×	✓	×	Log file analysis
RGCE	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	–
BUTCA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
OCR	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×	Other categories to be developed on customer request
Luxembourg Cyber Range	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	–
PAIDEUSIS	×	×	×	✓	×	×	×	✓	✓	×	×	×	✓	×	–
Tecnalia Cyber Range Laboratory	×	✓	✓	×	✓	×	×	×	×	×	×	×	✓	×	–
Airbus CyberRange	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	×	–
M&NTIS Platform	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	×	×	–
CYRIN	✓	×	×	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	IT and DevOps
Range365	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	–
CyTrONE	✓	✓	✓	✓	×	×	×	✓	×	✓	×	×	✓	×	–
Cybermentis	✓	×	✓	✓	×	×	×	×	✓	✓	✓	×	×	×	–
RangeForce Cyber Readiness Platform	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	×	✓	×	–
Cybels	✓	×	×	×	✓	×	×	✓	×	✓	✓	×	✓	✓	–
UNSW Cyber Range	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SimSpace Platform	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
CRACK	✓	✓	×	✓	✓	×	×	✓	×	×	×	×	×	×	Maritime Scenarios
Mizzou Cyber Range	×	×	✓	×	✓	✓	×	✓	✓	×	×	×	×	×	–
Ohio Cyber Range	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	–
Coliseum	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	–
DIATEAM Hybrid Cyber Range	✓	×	✓	✓	✓	×	×	✓	✓	×	✓	×	×	✓	–
CybExer Cyber Range	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	×	Best practice training, CSIRT processes, Blockchain Essentials, Others to be developed on customer request
Cyberbit Range	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	–
AIT Cyber Range	✓	✓	✓	✓	✓	✓	×	✓	✓	×	×	×	✓	×	–
CDeX	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	–

✓ = Scenario category available, × = Scenario category not available, N/A = No information provided, – = No additional information

attack mitigation but rather on the traceability and legal accountability of IT security incidents.

One of the most important things to consider when choosing a CR or a CR training programme is which skills you can train with a platform. The needs differ from organisation to organisation. Therefore, we asked which training categories are generally supported by a platform. A quantitative overview is shown in Fig. 20. Seven CRs also indicated support for further/other training types in free-text responses, though no new generalisable categories emerged. The results reveal two distinct groups of scenario categories:

1) Categories that are supported by well over 50% of the 38 CRs: IR Training, SOC Training, Threat Hunting, Forensics, Critical Infrastructure, Network and Malware Analysis, Linux/Windows Analysis, and Pentesting.
2) Training areas that are significantly less supported, including Internet of Things (IoT), MacOS analysis, mobile systems, malware development, and additional provider-specific topics. For these less-supported areas, careful provider selection is required to ensure availability of suitable content.

5) SUPPORTED TRAINING GROUPS

Table 14 and Fig. 21 show which training groups/teams can be trained in a CR or can participate in a CR training. Of the 41 CRs, 40 support blue teams and 37 red teams, confirming their central role in CR-based training. Only

TABLE 14. Available training groups.

Cyber Range	Green Team	White Team	Red Team	Blue Team	Transparent Team	Yellow Team	Purple Team	Grey Team
ICE&T	×	×	✓	✓	✓	✓	✓	✓
CySOP	×	✓	✓	✓	✓	×	✓	×
Immersive	✓	✓	✓	✓	✓	✓	✓	×
iTrust Labs	✓	✓	✓	✓	✓	✓	✓	✓
TELECOM Nancy Cyber Range	×	×	✓	✓	×	×	✓	×
Vigrid	✓	✓	✓	✓	✓	✓	✓	✓
SPHERE	✓	✓	✓	✓	×	×	✓	×
CENTS + RangeOS	✓	✓	✓	✓	✓	✓	✓	✓
Laokoon Attack XPerience	✓	✓	✓	✓	×	✓	✓	×
MCR	×	✓	✓	✓	✓	✓	✓	×
KYPO CRP	✓	✓	✓	✓	✓	✓	✓	✓
Cyber Simulation Center	×	×	×	✓	×	×	×	×
Cyrange	×	×	✓	✓	×	×	×	×
EDURange	✓	×	✓	✓	✓	✓	×	×
Virginia Cyber Range	×	×	✓	✓	×	×	×	×
CRATE	✓	✓	✓	✓	✓	✓	✓	✓
RGCE	✓	✓	✓	✓	✓	✓	✓	✓
BUTCA	✓	✓	✓	✓	✓	✓	✓	✓
OCR	✓	✓	✓	✓	✓	✓	✓	✓
Luxembourg Cyber Range	✓	✓	✓	✓	✓	✓	✓	×
PAIDEUSIS	×	×	✓	✓	×	×	×	×
Tecnalia Cyber Range Laboratory	×	✓	✓	✓	×	×	×	×
Airbus CyberRange	✓	✓	✓	✓	✓	✓	✓	✓
M&NTIS Platform	×	✓	×	✓	×	×	✓	×
CYRIN	✓	✓	✓	✓	✓	✓	✓	✓
Range365	✓	✓	✓	✓	✓	✓	✓	✓
CyTrONE	×	×	✓	✓	×	×	×	×
Cybermentis	×	×	×	✓	×	×	✓	×
RangeForce Cyber Readiness Platform	×	×	✓	✓	×	×	✓	×
Cybels	✓	✓	✓	✓	✓	✓	✓	✓
UNSW Cyber Range	×	✓	✓	✓	✓	×	✓	✓
SimSpace Platform	✓	✓	✓	✓	✓	✓	✓	✓
CRACK	✓	✓	✓	✓	×	✓	×	×
Mizzou Cyber Range	✓	×	×	×	×	×	×	×
Ohio Cyber Range	✓	✓	✓	✓	×	×	✓	×
Coliseum	✓	✓	✓	✓	✓	✓	✓	✓
DIATEAM Hybrid Cyber Range	✓	✓	✓	✓	✓	✓	✓	✓
CybExer Cyber Range	✓	✓	✓	✓	✓	✓	✓	✓
Cyberbit Range	✓	✓	✓	✓	✓	×	✓	✓
AIT Cyber Range	✓	✓	✓	✓	×	✓	✓	✓
CDeX	✓	✓	✓	✓	✓	✓	✓	✓

✓ = Training scenarios for participation available, × = Training scenarios for participation not available

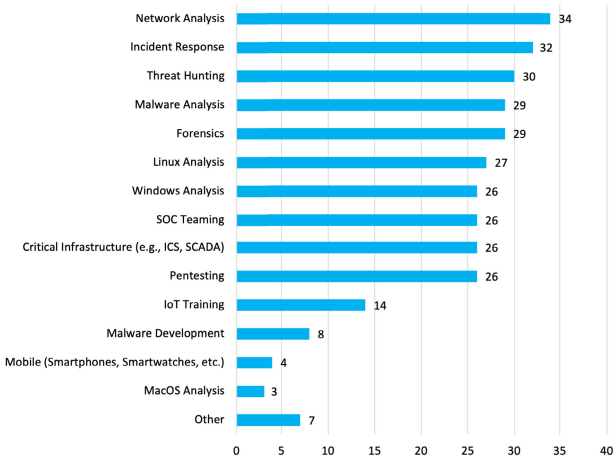


FIGURE 20. Cyber range preconfigured scenario categories (N = 38).

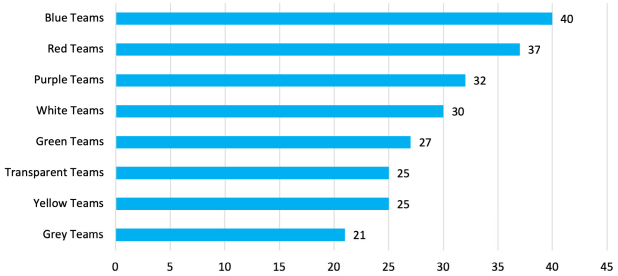


FIGURE 21. Cyber range training groups (N = 41).

the Mizzou CR does not support blue team training, while red team training is not offered by the Cyber Simulation Center, the M&NTIS Platform, Cybermentis, and again the Mizzou CR. This corresponds with findings in Section V-E, which indicate a slight emphasis on defensive over offensive training.

Beyond red and blue teams, 32 CRs support purple teams (combining elements from offensive and defensive

TABLE 15. Cyber range training scenario attack implementation and simulation.

Cyber Range	Attack Execution Options					Attack Execution Implementation
	None	Automated Attacker System	Manually Controlled Attacker System	Injects/ Poisoning	Attack Generator	
ICE&T	×	✓	×	✓	×	Remotely controlled live attacker system via orchestrator system playbooks; At least one dedicated attacker system per training environment
CySOP	×	✓	✓	×	✓	Dedicated attack VMs within a training environment
Immersive	×	×	✓	×	×	–
iTrust Labs	×	✓	✓	✓	✓	Attacking scripts either in iTrust Attack Desk tool, PLC code, Python, or any other preferred programming language
TELECOM Nancy Cyber Range	×	✓	✓	×	✓	Manual execution by the red team
Vigrid	✓	×	×	×	×	–
SPHERE	×	×	×	×	✓	–
CENTS + RangeOS	×	✓	✓	✓	✓	Advanced Persistent Threat playbooks define the execution manually, automated, or as combination of the two; Attacks organised along the MITRE ATT&CK Framework, Caldera campaigns, or basic Kali Linux, Metasploit discrete actions
Laokoon Attack XPerience	×	✓	✓	✓	×	Either manual execution by red team or automated via injection points
MCR	×	✓	✓	✓	✓	Automated execution via attack generator based on XML scripts; Manual live execution via Kali OS machines in simulated LAN and WAN of the training environment
KYPO CRP	×	✓	✓	✓	×	Either manual execution by red team or automated via homebrewed tool or attacking script
Cyber Simulation Center	×	✓	✓	✓	×	Predefined attack paths executed by the trainers; Live intervention based on the trainees speed and knowledge
Cyrange	✓	×	×	×	×	–
EDURange	✓	×	×	×	×	–
Virginia Cyber Range	×	×	✓	×	×	–
CRATE	×	✓	✓	✓	✓	CRATE's Sved tool creates attack graphs that are pre-programmed and to be executed automatically; Attack execution via remotely controlled, heavily modified Kali Linux VMs; Automated Sved attack graph generation via ML based tool 'Lore'
RGCE	×	✓	✓	✓	✓	Attacks defintion based on threat actors' TTPs (techniques, tactics and procedures); Manual execution by in-house red team; Combined attacks form a larger operation or mission
BUTCA	×	✓	✓	✓	✓	In house development
OCR	×	×	✓	✓	×	–
Luxembourg Cyber Range	×	✓	✓	✓	×	Manual execution by the red team
PAIDEUSIS	✓	×	×	×	×	–
Tecnalia Cyber Range Laboratory	×	×	✓	×	×	–
Airbus CyberRange	×	✓	✓	✓	✓	Definition of 'actions' (= one-step attacks) and/or 'scenariorized actions' (= chains of actions that can be executed in sequence and/or in parallel); Either automated execution via scheduling or manually
M&NTIS Platform	×	✓	✓	×	×	Automated execution via redteam engine that allows to gather and analyze outputs from previous attack steps to trigger next attack steps; The engine system is based on attack graphs
CYRIN	×	×	×	✓	×	Built-in CYRIN Agents or attack scripts.
Range365	×	✓	×	×	×	Attacking scripts using various programming / scripting languages and interacting with the Metasploit Framework; All attacks aligned to the MITRE ATT&CK Framework with some specifically crafted to emulate Advanced Persistent Threat groups
CyTrONE	×	✓	✓	✓	✓	Automated execution via Cyber Range modules during the scenario setup; Scenario progression management module CyPROM enables additional live attacks
Cybermentis	×	✓	✓	✓	×	Automated execution of internally developed, predefined scenarios based on the Caldera framework
RangeForce Cyber Readiness Platform	×	✓	×	×	×	Automated execution of internally developed, predefined scenarios
Cybels	×	✓	✓	✓	✓	Automated execution based on Caldera or manual execution via Cyber Range engineers
UNSW Cyber Range	×	✓	✓	✓	✓	–
SimSpace Platform	×	✓	×	×	×	Automated execution of internally developed, predefined scenarios
CRACK	×	×	×	×	✓	Automated execution via programmable agents on live attacker systems
Mizzou Cyber Range	×	×	×	✓	×	Execution via publicly available attack tools and customised scripts to automate them
Ohio Cyber Range	×	✓	✓	✓	✓	Automated/scheduled execution; Manual execution by red team used in large exercises
Coliseum	×	✓	✓	✓	✓	Automated execution via Ghosts simulated attackers, IaC, or third party tool integration
DIATEAM Hybrid Cyber Range	×	✓	✓	✓	✓	Automated execution via third-party commercial tools like Adversary Emulation Plan software; Manual execution for advanced cyber exercises
CybExer Cyber Range	×	✓	✓	✓	✓	Gradually escalation of pre-developed attack scenarios over time, with each new phase introducing new TTPs aligned with the MITRE ATT&CK framework
Cyberbit Range	×	✓	✓	✓	×	Automated execution of predefined attacks via Metasploit framework and scripts at the beginning of the training scenario
AIT Cyber Range	×	✓	✓	✓	✓	Either manual execution by the red team or automated via attack engineor attacking scripts
CDeX	×	✓	✓	✓	✓	Either manual execution by red team in red vs. blue scenarios or fully-automated execution of predefined attack kill chains via CDeX Agent

✓ = Possible, × = Not possible, N/A = no information provided, – = No supplementary information

roles), 30 white teams, 27 green teams, 25 yellow teams, 25 transparent teams, and 21 grey teams. White, green, and yellow teams are generally considered supportive teams that contribute to training execution rather than being the primary training focus. These teams can be part of a training scenario, either as part of the training provider or part of the personnel being trained. It is reasonable to assume that CRs who selected these teams in the response options of the questionnaire intend them as integral components in facilitating training exercises.

Grey and transparent teams, however, represent specialised roles and are the least commonly supported. Their inclusion

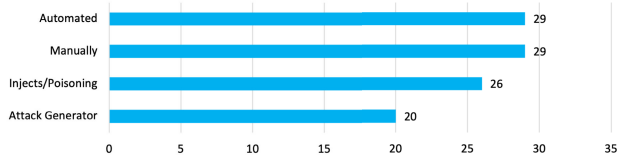


FIGURE 22. Cyber range attack execution features (N = 37).

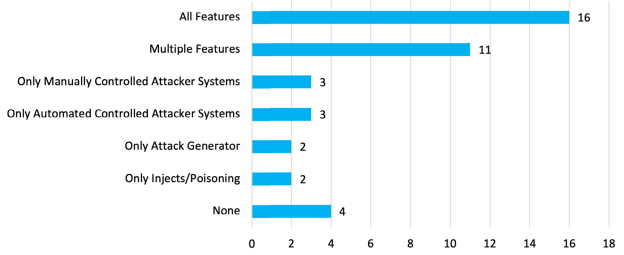


FIGURE 23. Cyber range attack execution support (N = 41).

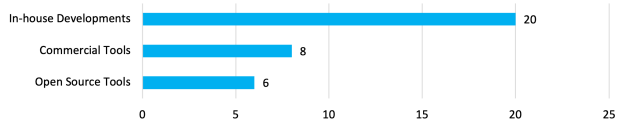


FIGURE 24. Cyber range network traffic generation implementation (N = 31).

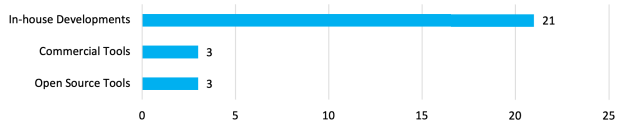


FIGURE 25. Cyber range user simulation implementation (N = 24).

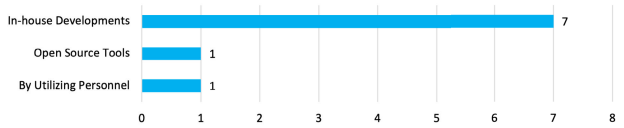


FIGURE 26. Cyber range defender simulation implementation (N = 9).

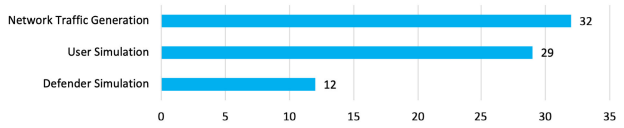


FIGURE 27. Cyber range network traffic simulation type (N = 41).

often reflects special use cases and must be considered when selecting a specific CR platform.

Overall, the data illustrates the broad spectrum of team-based training models supported by CRs, with red, blue, and purple teams being the most prevalent, and supportive or specialised teams being integrated to varying degrees. Nevertheless, the data in Table 14 shows that CR training primarily focuses on technical exercises for defenders and attackers.

6) ATTACK IMPLEMENTATION IN TRAINING SCENARIOS

To assess the learning effectiveness of defensive CR training, it is essential to understand how cyberattacks are implemented in training scenarios. Depending on the implementation, realism, effort, or achievable objectives vary. However, also the automation potential differs. The corresponding results are presented in Table 15.

Four CRs (Vigrid, Cyrange, EDURange, and PAIDEUSIS) do not implement an attack execution or simulation feature. Among the remaining 37, 29 use automated live attacker systems (e.g., Kali or ParrotOS controlled via orchestration), and 29 support manually controlled live attacker systems. Attack generators are implemented in 20 CRs, while 26 simulate attacks via injects/poisoning on target systems. Fig. 22 provides an overview of these numbers.

Most CRs support multiple attack execution techniques, while 16 use all four. However, 10 CRs are based on a single method. For example, Immersive, the Virginia CR, and the Tecnalia CR utilise only manual live attacker systems. Range365, RangeForce, and SimSpace rely solely on automated attacker systems. SPHERE and CRACK use an attack generator, and CYRIN and the Mizzou CR use injections/poisoning. Fig. 23 summarises this distribution. In total, 27 CRs combine two or more methods, enabling flexible, scenario-specific attack execution. For instance, live attacker systems can be used to create realistic traces, while attack generators add persistent background activity.

Live attacker systems – regardless of whether automated or manually controlled – are the most common, used by 33 CRs. In contrast, SPHERE, CRACK, CYRIN and the Mizzou CRs rely exclusively on attack generators or injects, which are methods that generate less realistic attacks for complex CR training scenarios with structured storylines. Overall, however, our results show a clear emphasis on realism in the execution of cyberattacks.

Automation also plays a central role in CR attack execution. Of the 37 CRs using at least one method, 34 support some level of automation. Only Immersive, the Virginia CR, and the Tecnalia CR depend solely on manual attack execution. This highlights attack automation as a dominant trend in CR training, ensuring scalable and dynamic attack execution across different training scenarios.

7) SIMULATION FEATURES IN TRAINING SCENARIOS

Beyond attack execution, features such as network traffic generation, user simulation, and defender simulation significantly influence the realism, scope, and complexity of CR training. The corresponding data is summarised in Table 16.

TABLE 16. Cyber range training scenario simulation and injection features.

Cyber Range	Network Traffic Generation	User Simulation	Defender Simulation
ICE&T	×	Adjustable powershell scripts that operate on a randomised temporal basis	×
CySOP	×	VM-templates which include specified user actions to be simulated at start-up or delayed	×
Immersive	×	×	×
iTrust Labs	Benign traffic & noise scripts injection	CLI and GUI automation tools	Implemented through detection and defence technologies
TELECOM Nancy Cyber Range	Keysight Breaking Point & Airbus Network Generator	Airbus LADE automation agent	×
Vigrid	GNS3 extensions through API allow jitter, packet loss, and latency adjustments	×	×
SPHERE	×	–	–
CENTS + RangeOS	Carnegie Mellon's Gh0st framework	Randomly operating micro services	×
Laokoon Attack XPerience	Benign network traffic injection by the provider	Provider-only feature	×
MCR	In-house development	In-house development	×
KYPO CRP	Third-party Open Source software	Third-party Open Source software	×
Cyber Simulation Center	×	×	×
Cyrange	×	×	×
EDURange	Integrating scripting hosts to the training environment	×	×
Virginia Cyber Range	×	×	×
CRATE	CRATE's Sved (Scanning, Vulnerabilities, Exploitation and Detection) tool	Crate Action Framework (CAF), which enables codeable user actions	×
RGCE	In-house development	Adjustable end-point based agents	×
BUTCA	In-house development	In-house development	In-house development
OCR	Scripts and network traffic generator devices	In-house development	By utilising personnel; subject to training planning
Luxembourg Cyber Range	Keysight Breaking Point	×	×
PAIDEUSIS	×	×	×
Tecnalia Cyber Range Laboratory	Available in some blue team exercises	×	×
Airbus CyberRange	Adjustable Airbus traffic generators & third-party support	Configuarble AI based Airbus user simulation tool with triggers based on time and or previous actions	Extendable automated defender actions, triggered based on time and/or previous actions
M&NTIS Platform	PCAPs replayed from specific nodes	Automated agentless user simulation relying on a catalogue of unitary user actions utilising KVM remote desktop capabilities (SPICE, VNC)	×
CYRIN	Adjustable traffic generators templates	Adjustable CYRIN agents	Adjustable CYRIN agents
Range365	External and internal traffic generators adjustable related to training scenario difficulty	Active Directory user emulation	×
CyTrONE	×	×	×
Cybermentis	×	×	×
RangeForce Cyber Readiness Platform	Benign network traffic injection by the provider	Provider-only feature	Provider-only feature
Cybels	×	Provider-only feature	×
UNSW Cyber Range	Keysight Breaking Point	In-house development	In-house development
SimSpace Platform	–	Configurable user models representing typical enterprise roles	×
CRACK	Custom agents deployed on training environment systems	Custom agents deployed on training environment systems	×
Mizzou Cyber Range	Adjustable attack script	×	×
Ohio Cyber Range	Keysight PerfectStorm & multiple Open Source tools	Custom scripts	×
Coliseum	Infrastructure as code functionalty & Third-party integrations	Infrastructure as code functionalty & Third-party integrations & Carnegie Mellon's Gh0st framework	Carnegie Mellon's Gh0st framework
DIATEAM Hybrid Cyber Range	Third-party commercial tool	Virtual User DIATEAM solution	×
CybExer Cyber Range	Keysight Breaking Point & Custom scripts from red team	Automated agentless user simulation enabling the creation of persona templates	Simulated defenders implemented through Ansible playbooks and adjustable by exercise organisers
Cyberbit Range	on-premise product: integrated and configurable network generator	Adjustable attack scripts	×
AIT Cyber Range	Provider-only feature	Provider-only feature	Provider-only feature
CDeX	Network traffic generator based on the CDeX Agent tool	CDeX Agent tool	CDeX Agent tool

× = There is no such feature, – = Feature available, but no concrete information provided

With 32 CRs supporting network traffic generation, this feature is the most commonly implemented simulation functionality. In-house developed tools or templates are used by 20 CRs, eight rely on commercial solutions (e.g., Keysight appliances), and six support Open Source tools. Support for Open Source and commercial tools was counted if (i) this was explicitly mentioned for one or the other, or if (ii) third-party tool use/integration or external tool use/integration was mentioned. Therefore, Range365 and Coliseum are listed for both commercial and Open Source tool usage/support. Three CRs (AIT, Laokoon, and RangeForce) limit the traffic generation feature to the provider, while the Tecnalia CR Lab did not specify implementation details. Fig. 24 summarises these findings.

Furthermore, a total of 29 CRs do have a user simulation functionality. In four cases (Laokoon, RangeForce, Cybels, AIT), only the provider can configure or run simulations. For SPHERE, no implementation details were given. Of the 24 CRs for which information is available, 20 use in-house developments (in some cases supplemented with external tools). Both, iTrust Labs and the Coliseum CR use commercial as well as Open Source tools. In contrast, KYPO relies on Open Source, TELECOM Nancy on commercial tools. Fig. 25 visualises these findings.

TABLE 17. Cyber range supervision features.

Cyber Range	Supervised Consumer Trainings	Train the Trainer	Custom Training Requests	Training Development Support
ICE&T	✓	✓	✓	N/A
CySOP	✓	✓	✓	✓
Immersive	✓	✓	✓	✓
iTrust Labs	✓	✓	✓	✓
TELECOM Nancy Cyber Range	✓	×	✓	✓
Vigrid	×	×	✓	×
SPHERE	✓	✓	✓	N/A
CENTS + RangeOS	✓	✓	✓	✓
Laokoon Attack XPerience	✓	×	✓	N/A
MCR	✓	✓	✓	✓
KYPO CRP	✓	✓	✓	✓
Cyber Simulation Center	✓	×	✓	N/A
Cyrange	✓	×	✓	×
EDURange	✓	✓	✓	✓
Virginia Cyber Range	×	×	✓	N/A
CRATE	✓	×	✓	✓
RGCE	✓	✓	✓	✓
BUTCA	✓	✓	✓	✓
OCR	✓	✓	✓	✓
Luxembourg Cyber Range	✓	✓	✓	✓
PAIDEUSIS	✓	✓	✓	N/A
Tecnalia Cyber Range Laboratory	✓	✓	✓	N/A
Airbus CyberRange	✓	✓	✓	✓
M&NTIS Platform	✓	✓	✓	N/A
CYRIN	✓	✓	✓	✓
Range365	✓	✓	✓	✓
CyTrONE	×	×	×	✓
Cybermentis	✓	✓	✓	N/A
RangeForce Cyber Readiness Platform	×	✓	✓	N/A
Cybels	✓	✓	✓	✓
UNSW Cyber Range	×	×	✓	×
SimSpace Platform	✓	✓	✓	✓
CRACK	✓	×	✓	N/A
Mizzou Cyber Range	✓	✓	✓	N/A
Ohio Cyber Range	✓	✓	✓	✓
Coliseum	✓	✓	✓	✓
DIATEAM Hybrid Cyber Range	✓	✓	✓	✓
CybExer Cyber Range	✓	✓	✓	✓
Cyberbit Range	✓	✓	✓	✓
AIT Cyber Range	✓	✓	✓	N/A
CDeX	✓	✓	✓	✓

✓ = Offered, × = Not offered, N/A = No training development other than by the provider possible

A defender simulation is the least common simulation feature, implemented by only 12 CRs. In the AIT CR and the RangeForce CR, the feature is provider-controlled. Together with SPHERE, these three provide no implementation details. Among the other nine CRs, seven use in-house solutions or developments. The Coliseum CR employs the Gh0st framework, and OCR uniquely uses no automated approach, but real personnel. Fig. 26 summarises these numbers. Fig. 27 additionally provides an overview of how many CRs support the respective simulation feature.

Fig. 24, Fig. 25, and Fig. 26 reveal a strong reliance on in-house development: 20 of 31 CRs use in-house solutions for traffic generation, and 21 of 24 for user simulation. For defender simulation, seven of nine implementations are also in-house. The low adoption rate of the defender simulation highlights the complexity to develop such a feature.

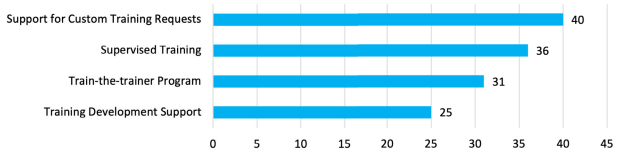


FIGURE 28. Cyber range supervision features (N = 41).

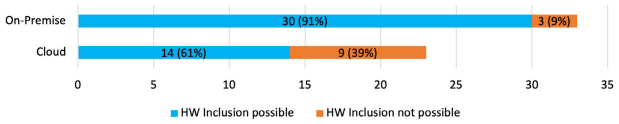


FIGURE 29. Hardware inclusion on-premise (N = 33) vs. Cloud (N = 23).

The varying adoption of commercial tools for implementing the different simulation functions is probably due to the complexity of the simulation functions themselves, their high need for adaptability and the general availability of commercial solutions. Network traffic generation is widely applicable beyond CRs, including for general network testing and performance analysis, resulting in the availability of several established commercial solutions. In contrast, user simulation requires more scenario-specific adaptations. For example, employee behaviour differs significantly between organisations, making in-house developments more preferable. Defender simulation is even more complex, as it depends on real-time attack context and reactive defence logic. This explains OCR's use of real staff and CRATE's ongoing development of an automated solution.

F. RESULTS REGARDING SUPERVISION AND SUPPORT FOR TRAINING DESIGN AND EXECUTION

Table 17 presents results for the accessibility category 'Supervision and Support for Training Design and Execution'. Fig. 28 provides a quantitative overview on the supported supervision features among CRs.

The results reflect a general emphasis on guided learning experiences. Thereby, a majority of 36 CRs offers supervised training. Only Vigrid, the RangeForce Cyber Readiness Platform, CyTrONE, the Virginia CR, and the UNSW CR have no such offer. Train-the-trainer programs are available in 31 CRs. The 10 CRs that do not provide such programs all focus primarily on delivering CR training, suggesting a strategic decision to concentrate resources on core offerings. Each platform must consider whether it has the necessary staff and whether resources should be committed to an additional, highly resource-intensive training programme.

Notably, Vigrid and CyTrONE, as Open Source platforms, lack commercial training components, which explains the absence of trainer education. In contrast, KYPO CRP demonstrates that Open Source CRs and structured training are not mutually exclusive.

TABLE 18. Cyber ranges hardware inclusion features.

Cyber Range	Hardware Integration		OT Support						Trainee Workstation Support
	On-Premise Product	Cloud Product	On-Premise Product			Cloud Product			
			Virtual	Physical	Other	Virtual	Physical	Other	
ICE&T	via OSI layer 2 VPN; Physical attachment via Ethernet-switch	N/A	✓	✓	–	N/A	N/A	N/A	×
CySOP	Depending on hardware and deployment; by using extra network segments	N/A	×	×	–	N/A	N/A	N/A	✓
Immersive	N/A	via VPN	N/A	N/A	N/A	×	×	–	✓
iTrust Labs	Includable: PLCs, computers, IoT devices, etc.	+	✓	×	Cyber twins, physical testbeds	✓	×	–	✓
TELECOM Nancy Cyber Range	via physical network interface	N/A	×	✓	–	N/A	N/A	N/A	✓
Vigrid	via physical + corresponding virtual network interface (one/VLAN), which are bound to GNS3 projects; Limited only by Linux kernels and OpenVSwitch	N/A	✓	✓	–	N/A	N/A	N/A	✓
SPHERE	+	N/A	✓	×	–	N/A	N/A	N/A	×
CENTS + RangeOS	via Hardware-in-the-Loop on OSI layer 2 & 3	via VPN	✓	✓	Bridge/switch for physical integration	✓	✓	–	✓
Laokoon Attack XPerience	via Ethernet or USB; Different OT Protocols like modbus supported	×	✓	✓	–	×	×	–	✓
MCR	via API that is capable to connect ICS/OT training environments	N/A	✓	✓	via API	N/A	N/A	N/A	✓
KYPO CRP	N/A	via VPN	N/A	N/A	N/A	✓	✓	–	✓
Cyber Simulation Center	×	N/A	×	×	–	N/A	N/A	N/A	✓
Cyrange	via host network interfaces	N/A	×	×	–	N/A	N/A	N/A	×
EDURange	×	Inclusion method depending on the cloud provider	×	×	–	×	×	–	✓
Virginia Cyber Range	usually via Ethernet or USB	×	N/A	N/A	N/A	×	×	–	×
CRATE	via Ethernet and other buses (e.g., serial or USB if connected to an Ethernet device)	N/A	✓	✓	–	N/A	N/A	N/A	✓
RGCE	Includable: PLCs and field devices, medical devices, critical infrastructure systems, energy production systems	N/A	✓	✓	–	N/A	N/A	N/A	×
BUTCA	N/A	via in-house development	N/A	N/A	N/A	✓	✓	–	✓
OCR	via physical access to VLANs (both optical and copper); Additional custom integration development offered	N/A	✓	✓	–	N/A	N/A	N/A	✓
Luxembourg Cyber Range	via physical Ethernet-switch	N/A	✓	✓	–	N/A	N/A	N/A	✓
PAIDEUSIS	via USB ports of the server or, if supported by the device, by Ethernet connection	N/A	×	×	–	N/A	N/A	N/A	✓
Tecnalia Cyber Range Laboratory	offered just in blue team exercises by connection to the 'Primary Substation lab'	N/A	✓	✓	–	N/A	N/A	N/A	✓
Airbus CyberRange	via Ethernet-switch; For usage over a public network, a "remote switch" is offered	via 'remote switch' which allows a secure connection over the Internet	✓	✓	Remote integration via 'remote switch'	✓	✓	Remote integration via 'remote switch'	✓
M&NTIS Platform	via a dedicated network interface, required to attach an external device	×	×	×	–	×	×	–	✓
CYRIN	via VPN	via VPN	✓	×	via VPN	✓	×	via VPN	✓
Range365	N/A	customers network segment via VPN	N/A	N/A	N/A	✓	✓	–	×
CyTrONE	×	×	×	×	–	×	×	–	×
Cybermentis	N/A	×	N/A	N/A	N/A	×	×	–	✓
RangeForce Cyber Readiness Platform	N/A	×	N/A	N/A	N/A	×	×	–	×
Cybels	via USB and Ethernet; Military material depending on connector availability	N/A	✓	✓	–	N/A	N/A	N/A	×
UNSW Cyber Range	Depending on hardware (e.g., USB pass-through or Ethernet)	×	×	✓	–	×	×	–	×
SimSpace Platform	via Hardware-in-the-Loop	via Internet proxy or directly in the datacenter with management possible over the SimSpace portal	✓	✓	via OT Kits (= miniturised system versions)	✓	✓	via OT Kits (= miniturised system versions)	✓
CRACK	via physical Ethernet connections or through OSI layer 2 VPN	N/A	✓	✓	–	N/A	N/A	N/A	×
Mizzou Cyber Range	N/A	×	N/A	N/A	N/A	×	×	×	✓
Ohio Cyber Range	via Hardware-in-the-Loop	N/A	✓	✓	–	N/A	N/A	N/A	✓
Coliseum	via physical Ethernet connections or through OSI layer 2 VPN	via VPN	✓	✓	–	✓	✓	–	✓
DIATEAM Hybrid Cyber Range	via hybrid port (Ethernet/WiFi/USB/4G/5G/.....)	N/A	✓	✓	–	N/A	N/A	N/A	✓
CybExer Cyber Range	On-Site: via Ethernet-switches; Remote: via pre-configured VPN box (OSI Layer 2 or 3); Hardware to be included in specific network segments within the training environment or within the simulated Internet	via VPN	✓	✓	–	✓	✓	–	✓
Cyberbit Range	Only for on-premise; via Ethernet	×	✓	✓	–	✓	×	–	✓
AIT Cyber Range	Depending on hardware; via Ethernet, sometimes with a protocol and media transformation	Depending on hardware; via Ethernet, sometimes with a protocol and media transformation	✓	✓	–	✓	✓	–	✓
CDeX	any network capable device via configuration performed by the end user through the CDeX GUI	Only for private cloud	✓	✓	–	✓	×	Physical integration via private cloud	✓

✓ = Possible, × = Not possible, N/A = No such product, + = Possible, but no further information specified, – = No further information

Custom training requests are supported by 40 CRs. CyTrONE is the only exception, consistent with its role as a standalone Open Source platform rather than a service provider. Support for customers creating their own scenarios is available in 25 CRs. As 13 CRs do not allow custom scenario creation (see Table 12), they were excluded from this evaluation. The remaining CRs – Vigrid, Cyrange, and the UNSW CR – do not offer support, despite allowing own scenario creation. In these cases, the lack of support likely stems from their focus on research or Open Source distribution rather than commercial service delivery.

Overall, the results show that CRs with commercial or training-oriented goals tend to offer supervision, trainer education, and scenario support, while Open Source or academic platforms sometimes prioritise platform provision and research functionality.

G. RESULTS REGARDING INCLUDABLE PLATFORMS, SYSTEMS, AND SOFTWARE

For the accessibility category 'Includable Platforms, Systems and Software', three subtopics were examined: (i) Includable hardware which also targets OT, (ii) platforms, systems and software support, and (iii) the usual training environment architecture. The results are outlined in the following. Beyond the capabilities of the individual platforms and the general trends, these also provide insights into the extent to which cybersecurity training scenarios can be customised to meet certain client-specific needs (e.g., integrating OT for a critical infrastructure provider).

1) HARDWARE INCLUSION

Table 18 presents the capabilities of CRs to integrate hardware and OT devices in both on-premise and cloud-based setups. Regarding on-premise CRs, 30 of 33 support hardware integration ($\approx$ 91%), while only 14 of 23 cloud-based CRs ($\approx$ 61%) do. As visualised in Fig. 29, integration appears generally easier in on-premise CRs, where physical interfaces such as Ethernet ports are commonly used (20 CRs). Five CRs additionally support VPN-based access.

In contrast, among cloud-based CRs, only three report using physical interfaces, and seven rely on VPN tunnels, reflecting the challenges of remote hardware access in cloud environments. Overall, of all CRs – whether on-premise or cloud-based – only the Cyber Simulation Center, CyTrONE, Cybermentis, the RangeForce Cyber Readiness Platform and the Mizzou CR are not able to include hardware.

The inclusion of OT, however, is implemented by fewer CRs. Regarding the on-premise CRs, 26 offer the possibility. Thereby, 24 support the integration of virtualised OT devices and 23 the physical integration. Both are supported by 21 CRs. SPHERE, iTrust Labs, and CYRIN use virtualised OT only, or in the case of iTrust, cyber-physical twins can be used to depict physical testbeds. The TELECOM Nancy CR, and the UNSW CR, on the other hand, rely purely on the integration of physical OT. In Fig. 30, the support for these different implementations is visualised.

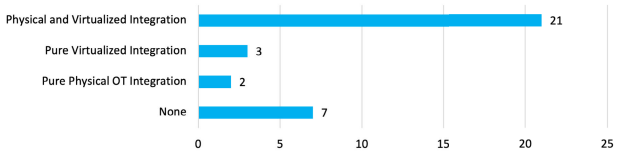


FIGURE 30. OT inclusion implementation on-premise (N = 33).

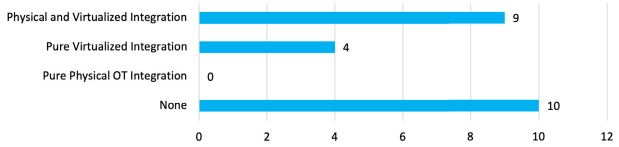


FIGURE 31. OT inclusion implementation cloud (N = 23).

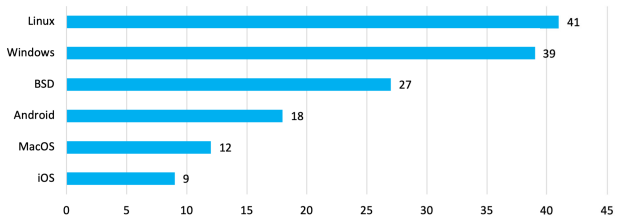


FIGURE 32. Supported OS (N = 41).

Among cloud-based CRs, 13 support OT integration: all offer virtual OT, and nine additionally support physical OT (see Fig. 31). The platforms of iTrust, CYRIN, Cyberbit, and CDeX support only virtual OT in the cloud. No cloud CR uses physical OT exclusively.

The lower adoption of OT integration overall reflects its specialised nature, which often requires support for industrial protocols (e.g., Modbus, Siemens). Additionally, OT integration is primarily relevant for training scenarios that focus on critical infrastructures or industrial production. This makes such integration less of a priority for general-purpose CRs.

There are 30 CRs which allow trainees to connect their own workstations directly into the training environment. While advantageous for advanced users which can use familiar tools then, this raises concerns, particularly in CRs without Internet access (see Table 6). In such cases, external devices may complicate the intended isolation of the training environment or unintentionally reintroduce Internet connectivity (e.g., via Internet forwarding and physical interfaces of the devices). This may be undesirable due to technical configurations such as the simulation of real Internet addresses or to contain data leakage or malware that may be included in training scenarios. Nonetheless, the widespread support reflects a high adoption rate of this functionallity.

Summarising, hardware integration is broadly supported in on-premise CRs, which can directly utilise physical interfaces, making hardware inclusion relatively straight-

TABLE 19. Cyber ranges platforms, systems and software support.

Cyber Range	OS Support	Proprietary Appliances Support	Trainee Tools Support	Forensic Images Support
ICE&T	Windows, Linux, Android, BSD	✓	On trainee request installers provided via a network share; For proprietary tools, licence required;.For whole appliances, contact before the training period required	Via tools installable in the training environments; Direct hardware access or hypervisor access is not possible
CySOP	Windows, Linux , BSD	✓	If the tools do not require Internet for installation; exception: custom scenarios that allow Internet	Via hypervisor access and VM-snapshots
Immersive	Windows, Linux, iOS, BSD, any OS with an AMI on AWS	✓	No restrictions	Via forensics tools supplied or tools configured by the customer
iTrust Labs	Windows, Linux, macOS	✓	Depends on training context	Depends on training needs
TELECOM Nancy Cyber Range	Windows, Linux, macOS (technically possible, but not authorised by Apple)	✓	Via virtual machines (OVF/QEMU) or containers (Docker)	Platform feature
Vigrid	Windows, Linux, macOS, Android, iOS, BSD	✓	No restrictions	Disk images via ZFS filesystem; Memory dump via QUEMU capabilities
SPHERE	Windows, Linux	✓	×	×
CENTS + RangeOS	Windows, Linux, macOS, Android, iOS, BSD, any OS provided as QCOW2 format	✓	Via the simulated Internet or directly on the endpoint	+
Laokoon Attack XPerience	Windows, Linux, Android, BSD	✓	In scenarios with Internet, no restrictions; In scenarios without Internet, e.g., via proxychains or at request provided by the trainers	Exportable after the training
MCR	Windows, Linux, Android, BSD	✓	×	×
KYPO CRP	Windows, Linux, BSD	✓	Via those trainee machines that have Internet	Via manual execution
Cyber Simulation Center	Windows, Linux, BSD	✓	Internet access individually grantable to allow tool downloads	Technically possible; Usually not part of training
Cyrange	Windows, Linux	✓	×	×
EDURange	Windows, Linux, BSD	×	×	+
Virginia Cyber Range	Windows, Linux , BSD	✓	Via (controlled) access to the Internet	×
CRATE	Windows, Linux , BSD	✓	Usually via custom VMs running on laptops connected to a segment in the trainee environment; For direct deployment, contact before the training period required	Via manual execution
RGCE	Windows, Linux, macOS, Android, BSD	✓	Under Cyber Range provider supervision	Platform feature & in special cases manually on the relevant system
BUTCA	Windows, Linux, macOS, Android, iOS, BSD	✓	Via in-house development	Platform feature
OCR	Windows, Linux, macOS, Android, iOS, BSD	✓	Depends on requirements	Via hypervisor; Custom solutions possible
Luxembourg Cyber Range	Windows, Linux, macOS, Android, BSD	✓	Via provided VMs	Via VMware hypervisor/Docker
PAIDEUSIS	Windows, Linux	✓	×	×
Tecnalia Cyber Range Laboratory	Windows, Linux	✓	×	Via manual execution by Cyber Range personnel
Airbus CyberRange	Windows, Linux, macOS, Android, iOS (via emulation), BSD, any OS supported by VMWare and integrated in a DOCKER container	✓	Any tool or appliance virtualisable under VMWare or provided as Docker container	Platform feature & user-deployed tools
M&NTIS Platform	Windows, Linux , BSD, Unix-based OSs	✓	Via executing ansible playbooks on targets; Wrapper API available	Platform feature
CYRIN	Windows, Linux, Android, BSD, any OS provided as VM-image	✓	×	Via hypervisor VM-snapshots
Range365	Windows, Linux	✓	Via Internet on the trainee SOC workstation	Via preinstalled forensic tools in the training environments
CyTrONE	Windows, Linux	✓	Via SSH transfer from the client machine used to connect into the training environments	Via manual execution by Cyber Range personnel
Cybermentis	Linux	×	Via Docker images specifically built for a training, but before the training period	×
RangeForce Cyber Readiness Platform	Windows, Linux, macOS	✓	×	×
Cybels	Windows, Linux , BSD	✓	For proprietary tools, licence required; Upload to the trainings environments only on request conducted by the trainers	Depending on system privileges, conductible directly on relevant systems
UNSW Cyber Range	Windows, Linux, Android, BSD	✓	×	×
SimSpace Platform	Windows, Linux, macOS, Android, iOS, BSD, any OS provided as OVA file	✓	No restrictions	Via VM-snapshots
CRACK	Windows, Linux, Android, BSD	✓	In scenarios with Internet, no restrictions	Via specific probes to be deployed on relevant systems
Mizzou Cyber Range	Linux	✓	Not intended as training materials specifically designed, but no restrictions	Manually on the relevant system
Ohio Cyber Range	Windows, Linux	✓	×	+
Coliseum	Windows, Linux, macOS, Android, iOS, BSD	✓	Via direct connection of own devices to the range, or user rights on the target systems	Platform feature & manually on the relevant system
DIATEAM Hybrid Cyber Range	Windows, Linux, Android, BSD	✓	When authorised in the training (on-demand)	Platform feature
CybExer Cyber Range	Windows, Linux, macOS (special adjustments required, not offered by default) , Android, iOS (via official Apple emulator) , BSD, any OS supported by VMWare or (when deployed this way) the cloud provider	✓	No restrictions on the pre-prepared Windows and Linux servers provided to trainees; In blue teams scenarios also possible on all systems required to defend	Via scripts or playbooks directly on the relevant system
Cyberbit Range	Windows, Linux	✓	Only available on-premise	×
AIT Cyber Range	Windows, Linux, Android, iOS	✓	via Internet or already initially deployed when contacted before training	×
CDeX	Windows, Linux , BSD, any OS provided as VM-image, e.g., ECDIS (maritime navigational system), Firewall OSs	✓	Via Internet inside the training environment or sent via SSH/RDP	Disk image export via platform feature

✓ = Yes, × = No, + = Yes, but no further information specified

forward. In cloud-based CRs, integration is more restricted and technically complex usually due to the lack of direct hardware access. OT integration follows a similar pattern: 26 on-premise CRs support OT, compared to only 13 cloud-based CRs. On-premise platforms show greater flexibility, often supporting both virtual and physical OT. In contrast, cloud CRs rely predominantly on virtualisation, highlighting the infrastructural limitations of cloud environments for hardware-centric training scenarios.

TABLE 20. Cyber ranges common training environment architecture.

Cyber Range	VMs	Containers	Hardware	Other / Supplementary Information
ICE&T	✓	✓	✓	×
CySOP	✓	✓	✓	×
Immersive	✓	×	×	×
iTrust Labs	✓	✓	×	Different implementations, depending on the training content
TELECOM Nancy Cyber Range	✓	✓	×	Physical networks
Vigrid	✓	×	✓	Physical networks
SPHERE	✓	✓	×	×
CENTS + RangeOS	✓	✓	✓	Any network device (virtual or physical)
Laokoon Attack XPerience	✓	✓	✓	×
MCR	✓	×	×	×
KYPO CRP	✓	✓	✓	×
Cyber Simulation Center	✓	×	×	×
Cyrange	✓	×	×	×
EDURange	✓	✓	×	×
Virginia Cyber Range	✓	✓	×	×
CRATE	✓	✓	✓	×
RGCE	✓	✓	✓	Virtual & physical appliances, commercial & in-house built hardware and software
BUTCA	✓	✓	✓	×
OCR	✓	✓	✓	Cyber-physical integrations; Cyber Range federation in development
Luxembourg Cyber Range	✓	✓	✓	×
PAIDEUSIS	✓	✓	✓	×
Tecnalia Cyber Range Laboratory	✓	×	×	×
Airbus CyberRange	✓	✓	✓	External virtual or physical assets like OT
M&NTIS Platform	✓	✓	×	×
CYRIN	✓	×	×	×
Range365	✓	×	×	×
CyTrONE	✓	×	×	×
Cybermentis	×	✓	×	×
RangeForce Cyber Readiness Platform	✓	✓	×	×
Cybels	✓	✓	✓	OT PLCs & Firewalls
UNSW Cyber Range	✓	✓	✓	×
SimSpace Platform	✓	×	×	×
CRACK	✓	✓	✓	×
Mizzou Cyber Range	✓	✓	×	×
Ohio Cyber Range	✓	×	✓	×
Coliseum	✓	✓	✓	×
DIATEAM Hybrid Cyber Range	✓	✓	✓	×
CybExer Cyber Range	✓	✓	✓	Cloud services, integrations with production environments
Cyberbit Range	✓	✓	✓	Hardware devices only for on-premise
AIT Cyber Range	✓	✓	✓	×
CDeX	✓	×	✓	×

✓ = Included, × = Not included

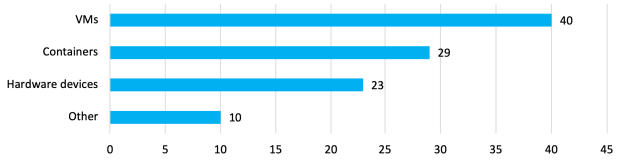


FIGURE 33. System types in training environments (N = 41).

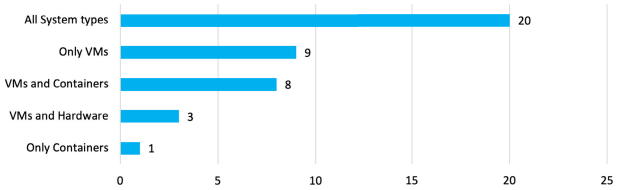


FIGURE 34. Standard training environment system types (N = 41).

2) PLATFORMS, SYSTEMS, AND SOFTWARE SUPPORT

In addition to hardware and OT integration, we assessed supported OSs, the inclusion of proprietary software, trainee software installation rights, and the ability to extract memory or disk images from training environments. The results are summarised in Table 19.

Fig. 32 shows that all CRs support to virtualise Linux-based OSs, and 39 also support Windows. Only Cybermentis and the Mizzou CR lack Windows support. This reflects the predominant OSs in the PC and server market. BSD-based systems can be virtualised by 27 CRs, Android by 18, MacOS by 12, and iOS by nine, making mobile and Apple OSs in general the least supported. M&NTIS and CDeX additionally used the free text field in the questionnaire to indicate support for two other 'non-standard' OSs: UNIX-based operating systems and maritime navigation systems.

Due to architectural constraints like ARM-based architectures for mobile OSs or licensing for macOS, these OSs are often emulated rather than virtualised, as stated by Cybexer and the Airbus CR (see Table 19). Nonetheless, 10 CRs report support for macOS virtualisation, and Cybexer and the TELECOM Nancy CR indicate that depicting these OSs is feasible with adjustments.

In 39 CRs, the inclusion of proprietary software or appliances is possible upon request. Thereby, 31 permit trainees to upload and install their own tools, though restrictions vary (see Table 19). In ICE&T, the Cyber Simulation Center, RGCE, Cybels, and the DIATEAM CR, such installations require assistance from CR staff. In most other cases, specific restrictions apply, dictating when, how, and on which systems software or tools can be downloaded and installed. Only Immersive, Vigrid, and SimSpace report no restrictions.

Furthermore, 32 CRs support to collect memory or disk images from systems inside the training environments. Interestingly, this is more than the 29 CRs that explicitly offer forensic training (compare Table 13). Again, the implementation details vary by platform, but the broad support for such functionality highlights its relevance across training types.

3) COMMON TRAINING ENVIRONMENT ARCHITECTURE

To understand the architecture of CRs and their training environments, it is important to analyse the types of systems that typically make up a training environment, not just the technical possibilities to integrate different systems. The corresponding results are summarised in Table 20.

With the exception of Cybermentis, which uses purely container-based training environments, 40 CRs use VMs in their training environments. Containers (e.g., Docker) are used by 29 CRs, often alongside VMs. This can be used to deploy containerised services within VM-based

TABLE 21. Cyber range training evaluation and learning outcomes features.

Cyber Range	Included LMS	Supported LMS	Progress Monitoring	Action Replay Feature
ICE&T	Moodle	✓	Automised measuring via orchestrator playbooks & remotely observable trainee desktops	×
CySOP	×	×	For threat scenarios, scored quiz at the end of a scenario; In newer releases, gated training scenarios where progress is stored incrementally during the scenario run; For CTFs: remote logging, detailed flag statistics, live dashboards, etc.& Mesh Central integration which allows monitoring multiple trainees, interacting with their PCs and recording the screen	×
Immersive	×	×	Scoreboard & After Action Reports	×
iTrust Labs	OpenEDX using Veyon, named 'GURU CPS'	✓	LMS & packet logs, etc.	Save
TELECOM Nancy Cyber Range	×	×	Manually via flags & quizzes	×
Vigrid	×	✓	×	Save
SPHERE	×	✓	Internal learning paths	×
CENTS + RangeOS	Moodle Workplace	✓	Competency frameworks that measure task performance	×
Laokoon Attack XPerience	×	×	Progress monitoring depending on the scenario; For example, amount of compromised hosts or detected attacks	×
MCR	×	×	Training station recordings & live monitoring by trainers via dedicated app	Save & Replay
KYPO CRP	In-house development; integration with other system in development	✓	Monitoring of network traffic, logs, or command line history	Save
Cyber Simulation Center	×	×	Included ticket system available for this purpose; Additional documentation, procured individually by the trainers	×
Cyrange	×	×	×	×
EDURange	×	×	Trainee command history & scored questions with trainee access to their score	Save
Virginia Cyber Range	×	✓	CTF progress can be monitored	×
CRATE	×	×	Incident reporting tool "CRATE Exercise Control" for trainee teams [8] & mostly monitored blue team systems that can be supervised in Elastic Search & Sved-tool self-action reports for the red team	×
RGCE	In-house development	×	In-house developed exercise management system	Save
BUTCA	In-house development	✓	in-house development	Save & Replay
OCR	In-house development (limited)	✓	Stateful team/progress monitoring and/or CTF flag checks; Custom solutions possible	Save
Luxembourg Cyber Range	In-house development	✓	Built in scoring- & awareness-tools and built in monitoring-tools	×
PAIDEUSIS	In-house development, provided with the platform	×	CTF flag checks	×
Tecnalia Cyber Range Laboratory	×	✓	In blue team exercises through integrated Root the Box [9]; In red team confrontation exercises via screen-sharing of each trainee to a video wall; In online red team exercises via VNC (only access method to training environments then) stream monitoring	×
Airbus CyberRange	Separately offered in-house developed LMS module	✓	Built in measurement KPIs, such as, but not limited to, progress tracking, point allocation, success rate, etc. & statistics on user progress provided by the LMS module	Save
M&NTIS Platform	×	✓	Measurements on the detection & response actions to live attack steps for tracking blue team progress	×
CYRIN	Moodle	✓	CYRIN Agent system monitors user actions and progress to completion	Save
Range365	In-house development named Cloud Range Performance Portal; centrally hosted & managed by the provider with multi-tenancy	×	Trainer workstation allows observing all candidate's SOC workstation desktops	Save & Replay
CyTrONE	Moodle	×	Overall training score based on scored questions included in the training scenario and provided via Moodle LMS	×
Cybermentis	Custom RLMS platform	×	Individual trainee KPI measurements for progress tracking, availableto the responsible manager	×
RangeForce Cyber Readiness Platform	Proprietary LMS	×	User activity, module completion, and team exercise success measurements	×
Cybels	×	✓	×	×
UNSW Cyber Range	×	×	×	×
SimSpace Platform	×	✓	Scoring system with measurements after each event in either individual or team environments	×
CRACK	×	×	Tracking via live scoring; Situational awareness web interface about the status of teams' activities in development	×
Mizzou Cyber Range	In-house development	×	Progress tracking through a database that keeps track of all the trainee activities & Trainees can perform a technical assessment with rank and awards based on their performance	Save
Ohio Cyber Range	×	✓	Through custom scripts, manual observation by instructors, and logs	Save
Coliseum	OpenOlat	✓	Via LMS and/or by trainee monitoring through the Cyber Range monitoring team	Save & Replay
DIATEAM Hybrid Cyber Range	Moodle	✓	×	Save
CybExer Cyber Range	In-house development, named 'Portal'	✓	Analysis mechanisms and metrics (real-time and post-exercise via database) dependent on use cases: • In Live Fire or Threat Hunting exercise, automated scoring of the blue team via: – Availability-Attacks Split (the 'split' between the availability of network systems of the blue teams and the successful red team attacks) calculated by a Gamenet Monitoring Agent (GMA) that monitors and scores the availability of different systems – VM revert penalty (penalizes participants with negative scoring in case they needed to revert VMs to a snapshot) – Performance Score (combined representation of successfully solved technical tasks), either automatically validated by GMA or manually by organisers – Indicators of Compromise (IoC) Sharing (represents the blue team's ability to create situational awareness and cooperate in sharing technical IoCs with others) – Reporting (scores articulation via situation reporting) – Special Score (represents the exercise management's ability to address any issues of fairness or unforeseeable technical events) – Team scoring and individual trainee scoring is thereby supported across all scoring categories • In Skills Testing and CTF based on a scoring of difficulty and skill level required to solve each single task, automatically validated by GMA or manually by organisers; Tasks can be grouped into different knowledge categories and in the use case of Skills Testing these are mapped to specific NICE KSAs • In training with hands-on labs practical, tasks are given and evaluated as done in the Skills Testing and CTF category	Save & Replay
Cyberbit Range	×	✓	Via reports, history of trainings and matching of content to MITRE ATTCK and NICE Frameworks	Save & Replay
AIT Cyber Range	In-house development	✓	In-house development	Save & Replay
CDeX	×	×	Automated granular scoring system implemented using CDeX Agent White Team actions	Save

✓ = Yes, × = No, Save = Actions can be saved but not replayed, Save & Replay = Actions can be saved and replayed

scenarios. Hardware integration is standard in 23 CRs. Fig. 33 provides an overview of these numbers. In addition, the free text option in the questionnaire was used to name possible further components of a training environment: the integration of federated training environments of other CRs (OCR) and cloud services (Cybexer).

[8] https://ieeexplore.ieee.org/document/9229649
[9] https://github.com/moloch–/RootTheBox

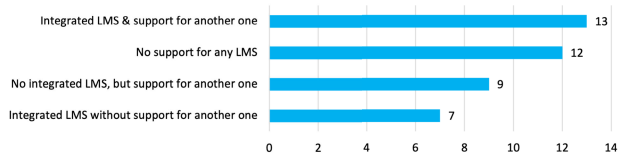


FIGURE 35. LMS support (N = 41).

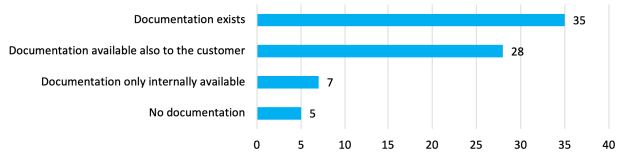


FIGURE 36. Platform documentation availability (N = 40).

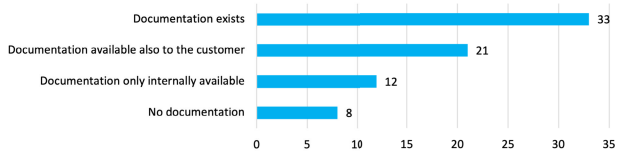


FIGURE 37. Orchestration documentation availability (N = 41).

Fig. 34 shows that 20 CRs combine VMs, containers, and hardware in their standard environments. Eight use VMs and containers, three VMs and hardware, and nine rely exclusively on VMs. Only Cybermentis uses containers exclusively. However, no CR relies solely on hardware.

Although 36 CRs support hardware integration (see Table 18), only 23 use it regularly in standard setups (see Fig. 33). This indicates that in 13 cases, the feature is available but not commonly used. VMs, however, are the predominant system type, used by 40 CRs, with nine using them exclusively. On the other hand, fully hardware-based environments are not standard in any of the surveyed CRs, and container-only setups are rare.

In total, 31 CRs employ mixed system types in their usual training environments (see Fig. 34). This flexibility enables scenario-specific modelling and supports varying levels of complexity. Combining VMs, containers, and hardware allows for enhanced realism and tailored training experiences.

H. RESULTS REGARDING TRAINING EVALUATION AND LEARNING OUTCOMES

For the accessibility category 'Training Evaluation and Learning Outcomes' all results are presented in Table 21. The results cover the use and support of LMSs, options for monitoring trainee and team progress in a CR training, and whether actions taken by trainees inside the training environments can be saved or replayed.

LMSs play an essential role in training evaluation. Fig. 35 shows that 20 CRs include an LMS, and 22 support integration of an external LMS. There are 12 CRs that do not support any LMS, nine allow external LMS integration, and seven CRs have an integrated LMS but do not allow additional integration. In summary, 29 offer LMS integration as an option. Thereby, the most included LMSs (11) are in-house developments. Seven CRs, however, rely on an Open Source LMS platform. Notably, customised LMSs (see Cybermentis) or proprietary solutions (see RangeForce) play a minor role.

Despite lacking LMS integration, 10 of the 12 remaining CRs still support trainee and team progress monitoring. The UNSW CR and Cyrange are the only exceptions. In total, 36 CRs implement monitoring functionalities (see Table 21), using either (i) quantitative, automated scoring or (ii) manual/qualitative evaluations such as reviews and after-action reports. Many CRs combine both approaches, but the implementation of monitoring features varies significantly between platforms.

However, unlike other areas of CR training, there is no predominant or standardised approach for monitoring and evaluation. Instead, each CR follows its own method, tailored to its specific training scenarios, which reflects the complexity and diversity of this task.

Only seven CRs support to fully save & replay trainee actions. Another 12 platforms allow at least saving without replay. The remaining 22 CRs do not offer such functionality. Both features aim to record and analyse trainee actions, but the replay capability enhances visualisation and review by allowing actions to be played back in sequence.

Saving all trainee actions requires accurate tracking of all actions, timestamps, file changes, and active processes. This sets high demands on storage capacity and monitoring capabilities, while ensuring that constant tracking does not distract or interfere with the training scenario. For the replay functionality, however, timestamps, file modifications, and active processes have to be additionally adjusted during playback. These challenges likely contribute to the limited availability of the feature across CRs, despite its potential benefits for post-training evaluation and analysis.

I. RESULTS REGARDING EASE OF ONBOARDING, MAINTENANCE, AND CUSTOMIZATION

The accessibility category 'Ease of Onboarding, Maintenance, and Customisation', was targeted by the questionnaire's final block. The results are presented in Table 22 and Table 23 and are elaborated in the following.

1) DOCUMENTATION, SUPPORT, AND TEMPLATES

This subcategory covers the availability of enterprise support, developer communities, platform and orchestration documentation, and system template libraries. Results are shown in Table 22.

There are 25 CRs – mainly platform vendors or providers of commercial services such as KYPO – that offer enterprise support. In contrast, the 16 CRs that do not offer this support are primarily focused on training delivery or

TABLE 22. Cyber range ease of onboarding – documentation, support, and templates.

Cyber Range	Enterprise Support	Developer Community	Platform Documentation	Scenario Orchestration Documentation	System Template Library	
					Availability	Extendability
ICE&T	×	×	✓	+	✓	By providing an OVA or Packer template for VMware vSphere to the Cyber Range personnel
CySOP	✓	×	✓	✓	✓	By importing VM-images supported by Proxmox VE as templates to the Cyber Range
Immersive	✓	✓	✓	+	✓	By creating and sharing templates of entire networks via built-in feature
iTrust Labs	✓	×	✓	✓	✓	By importing VM-images as templates to the Cyber Range
TELECOM Nancy Cyber Range	×	×	+	+	✓	By editing and saving existing VMs as templates
Vigrid	×	✓	✓	×	×	By importing VM-images supported by QEMU to the Cyber Range
SPHERE	✓	✓	×	+	✓	N/A
CENTS + RangeOS	✓	✓	✓	✓	✓	By editing and saving existing VMs as templates
Laokoon Attack XPerience	✓	×	+	+	✓	N/A
MCR	✓	×	✓	✓	✓	By creating custom templates in collaboration with the Cyber Range provider
KYPO CRP	✓	✓	✓	✓	✓	By creating custom templates in collaboration with the Cyber Range provider
Cyber Simulation Center	×	×	×	×	×	N/A
Cyrange	×	×	×	×	✓	×
EDURange	×	✓	✓	✓	✓	×
Virginia Cyber Range	×	×	✓	×	✓	N/A
CRATE	×	✓	✓	×	✓	Either VM-image import or by creating 'Managed Applications' that contain Ansible playbooks to be run on VMs during training environment deployment
RGCE	✓	×	✓	+	✓	By creating custom templates in collaboration with the Cyber Range provider
BUTCA	✓	×	+	✓	✓	In-house developed, built-in feature
OCR	×	✓	✓	✓	✓	Possible if created in accordance with the Cyber Range SDL (scenario definition language)
Luxembourg Cyber Range	✓	×	✓	✓	✓	By importing VM-images as templates to the VMWare Cluster
PAIDEUSIS	×	×	+	+	✓	N/A
Tecnalia Cyber Range Laboratory	×	×	×	×	×	N/A
Airbus CyberRange	✓	✓	✓	✓	✓	By importing VM-images as templates to the Cyber Range or editing and saving existing templates
M&NTIS Platform	✓	×	✓	+	✓	N/A
CYRIN	✓	×	✓	+	✓	Via CYRIN Exercise Builder tool
Range365	✓	×	✓	✓	×	New feature in development: Currently editing of systems via Vmware interface access
CyTrONE	×	×	✓	✓	✓	Details available in the user guide [10]
Cybermentis	✓	×	+	×	×	N/A
RangeForce Cyber Readiness Platform	✓	×	+	+	✓	N/A
Cybels	✓	×	✓	✓	✓	By editing and saving existing templates or request to the Cyber Range provider
UNSW Cyber Range	×	×	×	×	✓	By request to the Cyber Range provider
SimSpace Platform	✓	×	✓	✓	✓	By creating 'Clone Sources' that allow for entire Cyber Ranges to be save and stood back up
CRACK	×	×	+	+	✓	N/A
Mizzou Cyber Range	×	✓	✓	✓	✓	N/A
Ohio Cyber Range	✓	✓	✓	✓	✓	By providing an OVM or using a for this purpose provided test range environment for design and editing and have the Cyber Range team importing it
Coliseum	✓	×	✓	✓	✓	By importing VM-images that are compatible with VMWare or base images builtup through IaC (Ansible)
DIATEAM Hybrid Cyber Range	✓	×	✓	✓	✓	By creating topology patterns and cloning for integration
CybExer Cyber Range	✓	×	✓	✓	✓	Via the built-in feature vLab Manger (vLM) which relies on IaC and uses Ansible playbooks; User-friendly UI in development
Cyberbit Range	✓	×	✓	✓	✓	Only available on-premise
AIT Cyber Range	×	×	N/A	+	✓	N/A
CDeX	✓	×	✓	✓	✓	By importing any virtualised system into CDeX following the system import manual

✓ = Available, × = No such feature, + = Documentation exists, but is not available to the customer, N/A = No information provided

operate as Open Source platforms. A developer community, however, is only accessible for 11 CRs. These are either Open Source projects (see Table 2) or platforms developed by large enterprises, where a community-driven support ecosystem has naturally evolved or was established by the provider.

Documentation on the respective CR platform is available for 35 CRs, while five do not provide any, and the AIT did not respond. In 28 of 35 cases, this documentation can also be made available to customers. Documentation for the CR scenario orchestration, however, is available for 33 CRs. Only 21 of these enable customer access. For better comparison, Fig. 36 and Fig. 37 provide an overview of these numbers.

It is remarkable that allCRs that withhold (existing) platform or scenario orchestration documentation from customers focus primarily on training services. Giving customers the opportunity to operate the platform themselves and conduct training contradicts their core business model. However, the absence of documentation can complicate the platform maintenance and operational management. Yet five CRs (all training providers) lack platform documentation, eight lack orchestration documentation, and four lack even both.

A majority of 36 CRs provide a predefined system template library. The remaining five must create the systems for their training scenarios each time from scratch or reuse

[10]https://github.com/crond-jaist/CyTrONE

TABLE 23. Cyber range ease of onboarding – orchestration and automation tools.

Cyber Range	Training Infrastructure Setup Automation					Orchestration Software					Open Orchestration Software Support
	Packer	Terraform	OpenTofu	Heat	Other	Ansible	Puppet	Aria	SCOrch	Other	
ICE&T	✓	✓	×	×	–	✓	×	✓	✓	–	✓
CySOP	×	×	×	×	In-house development	×	×	×	×	In-house developed code	×
Immersive	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
iTrust Labs	×	×	×	×	Ansible	✓	×	×	×	–	✓
TELECOM Nancy Cyber Range	×	×	×	×	LADE automation system (via Airbus CyberRange)	×	×	×	×	LADE automation system (via Airbus CyberRange)	×
Vigrid	×	×	×	×	–	×	×	×	×	GNS3 client + Vigrid to clone etc.	✓
SPHERE	×	×	×	×	–	✓	×	×	×	–	✓
CENTS + RangeOS	×	×	×	×	In-house development, named RangeOS	✓	✓	×	×	Kubernetes	✓
Laokoon Attack XPerience	×	✓	×	✓	–	✓	×	×	×	–	✓
MCR	×	×	×	×	–	×	×	×	×	–	×
KYPO CRP	×	×	✓	×	–	✓	×	×	×	–	✓
Cyber Simulation Center	×	×	×	×	–	×	×	×	✓	–	✓
Cyrange	×	×	×	×	–	✓	×	×	×	–	×
EDURange	×	✓	×	×	–	×	×	×	×	Celery	✓
Virginia Cyber Range	×	✓	×	×	In-house developed provisioning backend	✓	×	×	×	–	×
CRATE	×	×	×	×	In-house development	✓	×	×	×	CRATE Core as orchestration software with Ansible integrated as component	✓
RGCE	×	×	×	×	Ansible, Poweshell, Bash	✓	×	×	×	–	✓
BUTCA	×	×	×	×	In-house development	×	×	×	×	In-house development	✓
OCR	×	×	×	×	In-house development, named OCR-Ranger & Ansible & further measures	✓	×	×	×	In-house development, named OCR-Ranger	✓
Luxembourg Cyber Range	×	✓	×	×	–	✓	×	×	×	–	✓
PAIDEUSIS	×	×	×	×	In-house developed scripts	×	×	×	×	In-house developed scripts	✓
Tecnalia Cyber Range Laboratory	✓	✓	×	×	–	×	×	×	×	–	✓
Airbus CyberRange	×	×	×	×	In-house developed tool with web interface and drag & drop functionality	×	×	×	×	In-house developed orchestrator	✓
M&NTIS Platform	×	×	×	×	In-house developed API for topology creation and initial VM configuration	✓	×	×	×	–	✓
CYRIN	×	×	×	×	Multiple Tools	×	×	×	×	Multiple tools	×
Range365	×	×	×	×	In-house developed software	×	×	×	×	Salt & in-house developed software	✓
CyTrONE	×	×	×	×	In-house development, named CyRIS	×	×	×	×	In-house development, named CyRIS	×
Cybermentis	×	×	×	×	–	×	×	×	×	–	×
RangeForce Cyber Readiness Platform	×	✓	×	×	–	✓	×	×	×	–	×
Cybels	×	×	×	×	–	×	×	×	×	–	✓
UNSW Cyber Range	×	×	✓	×	–	✓	×	✓	×	–	×
SimSpace Platform	×	×	×	×	Puppet, Ansible	✓	✓	×	×	–	✓
CRACK	✓	✓	×	×	–	✓	×	×	×	–	✓
Mizzou Cyber Range	×	×	×	×	Google Cloud API	×	×	×	×	–	×
Ohio Cyber Range	×	✓	×	×	–	✓	×	✓	×	–	✓
Coliseum	×	×	×	×	Ansible	✓	×	×	×	–	✓
DIATEAM Hybrid Cyber Range	✓	×	×	×	Vagrant	✓	×	×	×	–	✓
CybExer Cyber Range	✓	×	×	×	Ansible (mainly)	✓	×	×	×	–	×
Cyberbit Range	×	✓	×	×	–	×	×	×	×	VMware vCenter	×
AIT Cyber Range	✓	✓	×	×	–	✓	×	×	×	–	✓
CDeX	×	✓	×	×	–	×	×	×	×	In-house developed control and orchestration framework	×

✓ = Used, × = Not used, – = No supplementary information provided, N/A = No information provided

existing scenarios. In 27 CRs, the customers can expand the library. Cyrange and EDURange offer such libraries but without extension rights, and 12 platforms did not provide information regarding this matter. Vigrid and Range365, however, do not have a library for predefined systems, but Vigrid's architecture allows manual import and Range365 is developing such a functionality. Seven CRs – mostly training providers – require provider involvement to import templates. For them, the import of self-configured systems is more of a service than a platform feature. In contrast, vendors enable customers to extend libraries mostly via VM templates with defined compatibility requirements.

Summarising, the availability of documentation, support, and templates depends clearly on the strategic focus of each CR. In general, most CRs have sufficient documentation and system template libraries available. However, vendors emphasise self-service, onboarding, and customer autonomy, while training providers often prioritise scenario delivery. For training providers, assisting customers in the development of tailored training scenarios is more relevant than providing comprehensive documentation or self-service system templates. They may facilitate the integration of customer-specific templates, but do not aim to provide customers with extensive

resources for creating their own CR environments from scratch.

2) ORCHESTRATION AND AUTOMATION TOOLS

The final subtopic of our questionnaire examined orchestration and automation tools used in CRs, distinguishing between infrastructure setup automation and system and network orchestration. The results are summarised in Table 23, Fig. 38, and Fig. 39. Chef – a platform for server configuration and management with seamless cloud integration [93] – was included as an answer option in question *H010*. However, it was not used by any CR and is therefore not listed in Table 23. Detailed responses on orchestration and automation tools were provided by 40 CRs. Only Immersive did not provide any data.

Terraform is used by 11 CRs to set up the training infrastructure, six use Packer, and KYPO CRP and the UNSW CR use OpenTofu. Thereby, Laokoon uses OpenStack Heat and Terraform in conjunction.

Terraform is an infrastructure-as-code (IaC) tool for provisioning resources across various infrastructure providers [94], while OpenTofu is its Open Source fork maintained by the Linux Foundation [95]. Packer creates reusable, preconfigured system images (so-called 'golden images') to simplify environment setup [96]. Heat, however, is part of OpenStack and provides orchestration capabilities via its orchestration engine [97].

Proprietary or in-house solutions were reported by 12 CRs. Six CRs use Ansible, often in combination with other tools. OCR and others combine Ansible with custom solutions, despite Ansible being better suited to configuration management than infrastructure provisioning [98]. Other tools mentioned include Vagrant (DIATEAM), the Google Cloud API (Mizzou CR), and unspecified combinations of tools (CYRIN). Most noteable, seven CRs stated that the infrastructure setup is not automated at all.

Of the 33 CRs using automation tools for infrastructure setup, 21 rely on a single tool and 12 on multiple tools. Proprietary or in-house solutions are utilised by 10 of the CRs that use just a single tool, making up the majority of the 12 CRs with custom implementations (compare Table 23).

While their development and maintenance is resource-intensive, custom tools allow the complete integration of infrastructure automation processes. However, among CRs using a single tool, Terraform/OpenTofu is the most common freely available tool (8 CRs), making it the leading choice for all-around infrastructure setup with Open Source tools. At least nine CRs using multiple automation tools rely on combinations of public solutions. Additionally, the Virginia CR and OCR combine in-house and public tools, while CYRIN uses unspecified multiple tools.

There are 35 CRs that use orchestration tools for configuring their training environments: 26 use one, nine use multiple. Ansible is the predominant tool, named 22 times (15x as sole tool). Other tools include VMware Aria Orchestrator (3x),

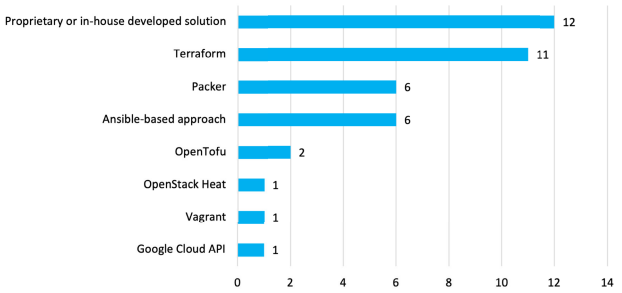


FIGURE 38. Cyber range infrastructure setup tools (N = 32).

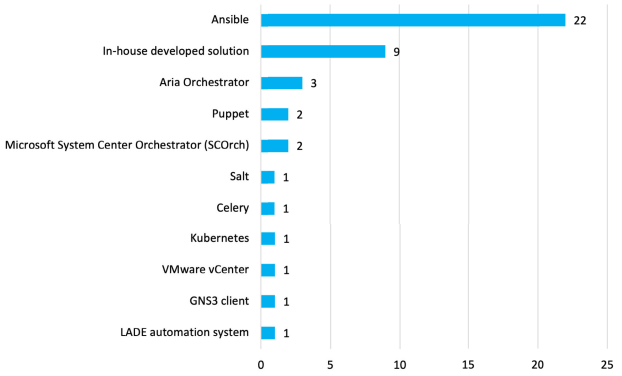


FIGURE 39. Cyber range orchestration tools (N = 34).

Puppet (2x), Microsoft System Center Orchestrator (SCOrch) (2x), Kubernetes, Salt, Celery, the VMware vCenter, the LADE automation system, and GNS3. The numbers are visualised in Fig. 39. However, 16 CRs use proprietary or in-house developed solutions. Thereby, OCR, CRATE, and Range365 combine these with Open Source tools. Five CRs do not use orchestration at all, while CYRIN again just stated to use 'multiple tools'.

Ansible is the most widely used orchestration tool, with 15 CRs relying on it exclusively. An interesting observation is that all six CRs that use Ansible for infrastructure setup automation also use it for training environment orchestration (see Table 23). However, as already mentioned, Ansible is not specifically designed for this purpose [98]. Still, there is an advantage of maintaining a single, familiar tool rather than requiring expertise in multiple different solutions.

Another observation is that the majority of CRs that invested in in-house development have done so comprehensively for both infrastrucutre automation and training environment orchestration. Of the 26 CRs using only one orchestration tool, nine use in-house-developments. Eight of these, however, also use custom infrastructure automation.

In total, 26 of 40 CRs support the integration of (external) open automation/orchestration tools. This includes some CRs that do not use them internally, highlighting that most platforms are flexible and customisable in this regard. However, Fig. 38 and Fig. 39 illustrate that publicly available tools are

the most commonly used solutions for both infrastructure setup automation and training environment orchestration. Nevertheless, 12 CRs rely on proprietary solutions for infrastructure automation, whereas 16 use proprietary or in-house-developed orchestration tools.

Twenty-one CRs of those that enable training environment orchestration already use publicly available tools. Five others – the Cyber Simulation Center, BUTCA, PAIDEUSIS, the Airbus CR, and Cybels – do not use them internally but allow integration. Conversely, seven CRs use public tools but block external integration, indicating limited flexibility. Restrictions in the integration of additional backend software can be linked to two factors: (i) training-focused CRs prioritise predefined experiences over extensibility, and (ii) proprietary CRs may intentionally limit customisation to retain platform control.

Overall, publicly available tools dominate CR automation and orchestration, with Ansible and Terraform/OpenTofu being the most widely used. Still, proprietary and in-house solutions continue to play a significant role, especially among CR vendors aiming for tight platform integration. Support for external orchestration and automation tools is common among flexible, vendor-oriented platforms but less so in training-focused or closed systems.

VI. ANALYSIS AND DISCUSSION

Most participants of this study are associated with the research & academia sector. This is a logical outcome given the initial qualitative literature review, which favours published academic data. Nonetheless, a significant number of CR providers also represent the industry sector. Notably, only seven participants had purchased a CR product and now offer training themselves. This suggests that most organisations that purchase a CR platform seem to use it rather for internal purposes, as only few of these could be identified. Last, but not least, prominent Open Source platforms and such that have a link to the military are also included in this survey. This diverse participant set – spanning academia, industry, military, training providers, platform vendors, and Open Source projects – enables well-grounded insights into the broader CR landscape.

A fairly general finding of this study is that the availability of certain features in CRs depends heavily on the provider's business model. The availability of documentation, support, and system templates clearly reflects the differing priorities among CRs. Platform vendors typically offer comprehensive resources to enable customers to develop and manage their own training scenarios. In contrast, training-focused CRs prioritise delivering predefined content and instead support customers by assisting in the development of tailored scenarios, rather than enabling full self-service. For example, capabilities such as adding custom systems or templates are treated more as a service provided to the customer than as a capability with which the customer could be equipped.

The following section outlines further key findings derived from the survey results presented in Section V. First, we describe the major trends that we have identified across different accessibility categories. This is followed by a discussion of how the CR landscape has evolved compared to descriptions in earlier research and whether earlier predictions could also be identified, reinforced or even confirmed.

A. TRENDS AND TOPICS IN THE CURRENT CYBER RANGE LANDSCAPE

With this survey and the collected data on all the CR features, we are able to provide a comprehensive analysis and insight into the current state of cyber security training via CRs. Three cross-cutting topics emerge throughout the different accessibility categories: (i) realism in training scenarios, (ii) automation, and (iii) the use of tools and software.

1) REALISM IN CYBER RANGES

The importance of realism in CR training becomes evident in the attack execution for the CR scenarios, the other simulation features, and the includable systems. Running cyberattacks via a dedicated attacker system produces the most realistic traces and artefacts for trainees – a feature implemented by 33 of the 41 CRs (see Table 15). Other features that make a training environment and the actions within more realistic, such as network and user simulation, are also implemented by the majority of platforms. However, defence simulation is less common due to high complexity (see Section V-E).

The choice of system types used within the training environment also influences realism. As shown in Section V-G, the integration of physical hardware is widespread. In 23 CRs, this is standard when designing a training environment. The integration of OT systems is also largely possible for both on-premise and cloud-based CRs (see Section V-E). However, the standard system type in the training environments is a VM.

In contrast to containers which do not run their own OS kernels but instead rely on the underlying OS of their system, VMs provide the abstraction of a physical machine with own virtual hardware and an independent OS [32]. VMs provide the image of an entire system, in contrast to containers, which can have different file systems and network configuration as a real hardware machine. However, the majority of CRs uses several system types, from hardware to VMs to containers, allowing the required level of abstraction to be selected and modelled for greater realism.

In summary, all these factors show how realism is implemented and increased in CRs. The large-scale implementation of realism-improving measures and further developments, such as defender simulation, show that realistic training is a core feature of CRs, and that there is a recognisable trend towards "active" training environments through the use of various simulation features.

2) AUTOMATION IN CYBER RANGES

There are two basic categories of automation in CRs. On the one hand, there is automation that serves purely

to make scenarios more realistic by providing additional digital artefacts and actions that would also be available in a productive network. This includes user simulation or network traffic-generation. On the other hand, there is also automation that simplifies and accelerates the creation of training environments and the execution of the training scenario. This includes (i) infrastructure setup automation, (ii) training environment system orchestration, (iii) a system template library, (iv) attack execution or simulation, and (v) defender simulation. However, defender simulation is less relevant and meaningful, as it is very complex to implement and/or in some cases is still under development (e.g., CRATE).

With regard to the first category, 32 of the 41 CRs use network traffic generation and 29 implement user simulation. These features are therefore widespread. However, as explained, they do not contribute to a more efficient, but rather to a more realistic execution of training scenarios. Automated attack execution is implemented in 34 CRs (compare Table 15), and as stated in Section V-I, 36 use a template library. Additionally, 33 CRs utilise automation for infrastructure setup, and 35 apply it to orchestrate training environment systems. This highlights that a clear majority of the 41 CRs uses automation for the setup and execution of CR training.

In total, 14 CRs lack at least one of the automation features that enable more efficient training scenarios. Among them, seven miss only a single function. Only Vigrid, Cybermentis, and the Tecnalia CR Laboratory reported to have three of the four relevant scenario automation capabilities not implemented. Although defender simulation could also enhance automation and efficiency, it was excluded from this analysis, as implementations are still in early stages.

However, there is not a single CR among the participants that does not use at least one automation capability at any point. The question for each CR is therefore much more about which automation has already been implemented or how far the automation process has progressed than whether automation is being used at all.

3) TOOLS AND SOFTWARE IN CYBER RANGES

Interesting observations can also be made about the tools used in CRs. This can be derived from the information on network traffic generation, user and defender simulation, infrastructure setup, and training environment orchestration.

For network traffic generation, 20 CRs rely on in-house developments, eight on commercial or proprietary tools or appliances, and six on Open Source or freely available tools (see Fig. 24). Regarding user simulation, 20 of the 24 CRs for which concrete information on the implementation of the feature is available are based on in-house developments.

Proprietary tools are used by three CRs, and another three CRs also use freely available tools (see Fig. 25). For the third simulation feature, the defender simulation, seven of the nine CRs also rely on in-house developments. Only once an Open Source tool is used for this, and in one case, even real personnel is involved (see Fig. 26). In-house developed solutions therefore dominate the simulation features in CRs. Freely available and proprietary tools are used less frequently.

In contrast, 27 CRs use Open Source or freely available tools for infrastructure setup, whereas only 11 rely on in-house developed solutions (see Table 23). For system orchestration, also a majority of 28 CRs uses Open Source or freely available tools. There are only nine in-house developments and seven proprietary tools or systems in use (see Fig. 39). However, as already analysed in Section V-I, eight of these nine platforms also use a self-developed solution for the infrastructure setup.

In infrastructure automation and orchestration, freely available tools are therefore dominant, whereas in-house developments are dominant in the implementation of simulation features. On the one hand, this can be explained by the broad availability of free and Open Source tools, such as Terraform, that were originally developed for automating and orchestrating cloud infrastructure. These tools are not only widely used in cloud environments, but are also well-suited for managing the complex infrastructures of CRs, making them an attractive choice for CR providers. On the other hand, the importance of interfaces for collaboration and resource sharing is increasing. For example, OCR and the Cybexer CR mention the keyword ''Cyber Range federation'' in their questionnaires. Clearly defined interfaces and, ideally, the use of the same tools are key to the implementation of such an interconnection of several CR instances.

Moreover, when new staff members are assigned to develop training courses for the CR, becoming acquainted with widely used tools and software – with extensive documentation and support – is far simpler than mastering an in-house solution used solely by the provider. The simulation of various user actions or network traffic, on the other hand, is not such a widespread use case and is only integrated on top of the scenario infrastructure and orchestration. This is probably the reason why the use of freely available tools for this purpose is less widespread so far compared to infrastructure and scenario orchestration.

B. DISCUSSION

In the following, we first discuss the technological evolution in the CR field. Therefore, we compare the technical capabilities of current CRs with descriptions from previous studies. Next, we examine the more general projections and outlooks from earlier research and how these fit with our findings.

1) REFLECTIONS ON TECHNOLOGICAL EVOLUTION

Compared to earlier studies, particularly Davis and Magrath [8] and Leblanc et al. [9], our findings highlight the maturing of the CR landscape. While they anticipated the increasing role of virtualisation, we confirm that virtualisation is now the dominant approach. However, contrary to the earlier belief that simulation might remain more flexible, our study shows that the combination of virtualised environments with real

hardware has become common practice, particularly in on-premise deployments. The integration of OT devices, both virtually and physically, is now widespread and reflects the recommendation of Holm et al. [21] to combine simulation with real hardware for high-fidelity scenarios.

Moreover, the evolution of tool availability and Open Source penetration testing distributions (e.g., Kali OS, the Metasploit framework or Exploit-DB) has enabled more realistic training environments. This confirms Davis and Magrath's projection that real attacks would replace simulations in many training scenarios [8]. However, the application purposes of a CR are pretty much the same as what Davis and Magrath [8] found: testing, training, and research and development.

Chouliaras et al. observed that CRs often support multiple domains and employ hybrid environments [11] – findings our study confirms and expands upon when querying focus areas and target groups. There are specialised CRs, but in general the platforms are designed to cover training for many different sectors. We also identify an increasing support for offensive training capabilities, automation tools like Ansible and Terraform, and a strong trend to let trainees access a CR platform via web/cloud-interface, reflecting broader developments in the sector. While Chouliaras et al. [11] focused only on which defensive courses and capabilities are offered by CRs, we found that most CRs also train or can train offensive capabilities of participants.

In Chouliaras study, OpenStack was identified as the dominant tool for deploying cloud infrastructure in CRs [11]. However, our data reveals a more diverse landscape: 14 platforms support Amazon AWS, eight each support Microsoft Azure and Google Cloud, and 11 rely on in-house or private cloud solutions. Several platforms state compatibility with any cloud provider, while others list additional support for niche platforms, such as OVH Cloud or Scaleway. While OpenStack is certainly present, it is typically deployed on top of other cloud infrastructures rather than serving as the primary cloud platform. We observe that, for example, VMware offerings or Proxmox are also used for this purpose.

Furthermore, with regard to automation tools, Chouliaras et al. [11] noted a strong emphasis on Ansible, Vagrant, and Packer, particularly in cloud-based deployments. Our findings indicate that such tools are now also widely adopted by on-premise platforms, reflecting an overall rise in automation practices. Especially infrastructure provisioning tools, such as Terraform and Packer, and tools such as Ansible, which are not dependent on the cloud but also work with local hypervisors, are widely used. The once clear distinction between cloud and on-premise CRs in terms of IaC tool usage has significantly blurred.

2) EVALUATION OF PREVIOUS PROJECTIONS AND OUTLOOKS

Our findings confirm and, in some areas, refine the projections made in previous studies regarding the technological development and operational focus of CRs. Holm et al. anticipated a growing reliance on virtualisation for ICS components, while also highlighting the challenges of emulating legacy field devices [21]. Our data validates this trajectory: the majority of on-premise CRs now support both virtual and physical OT integration, with virtualisation firmly established as the default approach, particularly in cloud-based platforms. However, physical OT integration remains prevalent, not due to technical limitations, but rather to enhance realism and reflect the cyber-physical nature of many training scenarios.

Yamin et al. [7] foresaw increasing automation across the CR lifecycle, a development our study can clearly confirm. Infrastructure provisioning and scenario automation are now widely implemented, both in cloud and on-premise settings. Similarly, the growing focus on training for ICS and OT environments, identified by Yamin et al. [7], is evident in our findings through the widespread support for OT integration. Their call for more realistic user simulation has also materialised: user simulation is now a common feature, and emerging support for defender simulation suggests the next stage of evolution. Furthermore, while Yamin et al. [7] proposed the use of cloud APIs for device integration, our data shows that practical implementations more often rely on hardware interfaces and VPN structures, particularly in hybrid on-premise environments.

Chouliaras et al. buildt upon the earlier observations by highlighting the critical need for comprehensive monitoring capabilities within CR platforms [11]. Our findings confirm this development, showing that most CRs now implement monitoring, albeit with a wide variety of tools and approaches. Compared to the more general listing of tools by Yamin et al. [7], the findings by Chouliaras et al. [11] reflect a clear transition phase, which our study continues by identifying both the prevalence of in-house monitoring solutions and the variety of tools currently in active use. Their observations about mixed training environments that combine virtualisation and hardware components are also validated in our data, where hybrid deployments are now common practice.

Previous concerns regarding the lack of educational support mechanisms have been partly addressed: most platforms now include at least basic learning evaluation features, such as integrated LMSs and assessment tools, though the implementation remains highly heterogeneous and standardised tools are still lacking. Thereby, we observe a reliance on in-house developments or customisations for both monitoring and learning evaluation – a state of the art that we also observe in user simulation tools.

Taken together, these developments suggest a consistent and measurable progression in the CR landscape. Reflecting from past work, CRs moved from conceptual proposals and limited implementations towards mature, hybrid, and highly customisable platforms with increasing focus on realism and automation. Educational support also appears to be a progressing topic, but has received less focus so far. This confirms several key assumptions in earlier work. However,

our study allows us to comment on the consolidation of CR tools and technologies. Unlike earlier solely literature-based studies, we identify predominant platforms (e.g., KVM, VMware), common automation and provisioning tools, and the widespread use of in-house developments for realism-enhancing features by providing updated, empirical insights and a comprehensive analysis of a broader and more diverse sample.

VII. CONCLUSION

In this section, we present the conclusions based on the survey data and its analysis. We state our contributions, name limitations, and provide an outlook and implications for future research. All the data from the survey is also made accessible to the public via the Open Data UniBw M platform[11] and our self-developed CR search engine.[12]

In this article, we identified eight categories that allow for the evaluation of the accessibility of cybersecurity training in CRs. These categories contain specific features, which allowed us to develop the CR feature ontology (see Fig. 1). This feature matrix can be used to compare CRs according to existing best practices, technical trends and lessons learned from current research.

Furthermore, we conducted a systematic literature review to provide an overview of the current state of the accessibility of cybersecurity training in CRs. We thereby examined training capabilities, along with technical and automation-related capabilities and features. As the information on the relevant features was not consistently available among the CRs identified in the literature review, a structured questionnaire was created, and a survey was conducted.

Our results present a comprehensive overview of the current CR landscape. We combine data from a systematic literature review with empirical data directly collected from the platform providers. The result is a detailed data set based on direct input from 41 verified operational CRs.

Therefore, our mixed-method approach enables a significantly more detailed and up-to-date analysis than prior work. This survey enables fine-grained comparisons and clear insights into tool adoption, implementation strategies, and platform capabilities. Detailed data on includable systems and software, training customisation, and scenario categories highlights how CRs enable tailored training solutions.

We identify differing strategic focuses among CR providers – ranging from fully customisable platforms offered by vendors to structured training services provided by training-focused CRs. Together with our publicly accessible 'CR search engine', this article facilitates broader access to detailed data on the accessibility of CR platforms, their features and the training they provide, supporting informed decision-making by practitioners and data access for researchers alike. Our study closes knowledge gaps, validates earlier projections, and offers new insights into the technological and pedagogical development of CRs for cybersecurity training.

However, this survey still faces some limitations. Despite covering a representative set of 41 CRs, detailed data from 31 additional relevant platforms is missing. Furthermore, our data set mainly includes platform vendors and self-developed CRs. Data from CR buyers is limited. It may be interesting to analyse their experiences and the adjustments they have made to the platforms in more detail in the future.

Government and military CRs are also only included to a limited extent, limiting insights into this sector's specific needs. Finally, with regard to the accessibility of cybersecurity training in CRs, we analysed the technical aspects of both the platform and the training content. Cost-related factors were not included. In addition, we queried the content of possible training courses, but did not analyse how the the CR training providers combine these to create their individual course offering. These are topics to further extend this study in the future.

Although further areas in the CR landscape can still be explored, this survey already reveals several developments and emerging needs that point to significant directions for future research in the field of CRs and cybersecurity training. In Section VI-A, we identified three major trends in current CRs, namely (i) an increasing emphasis on realism in training environments, (ii) the widespread adoption and expansion of automation, and (iii) the growing reliance on Open Source tools and orchestration software. However, these trends are tightly interlinked. Combined with further implications, this results in various areas that are likely to shape the evolution of CRs in the years to come. These are outlined in the following:

Federation and the Need for Standardisation: One key implication is the anticipated shift towards federated CRs. Early initiatives and projects already indicate the feasibility and growing relevance of CR federation [99], [100], which involves resource sharing, joint scenario development, distributed execution, and shared infrastructure across organisational or national boundaries. However, as our study shows, the current CR landscape is characterised by certain heterogeneity in tools, architectures, and interfaces. While the underlying platforms all rely on virtualisation and platform-independent automation and orchestration tools are on the rise, many topics in CR scenario execution and training evaluation are dominated by self-developed solutions. To enable federation on a broader scale, there is an urgent need for standardisation – not only of technical interfaces but also of scenario descriptions, evaluation metrics, and interoperability protocols.

Furthermore, the federation of CRs will necessitate advances in shared libraries for training models and data, as well as portable, reusable scenario components. This includes defining common scenario metadata, ensuring consistency in learning outcomes, and supporting seamless orchestration across federated platforms. From a research perspective, this opens up a wide range of topics related to secure data exchange, cross-domain access control, federated

[11] https://doi.org/10.60776/F1WOHD
[12] https://go.unibw.de/cyber-range-comparison

identity management, and network synchronisation. In this area the role of structured, not only machine-, but also human-readable documentation should also not be neglected. When porting a scenario or partial developments from one platform to another, human administrators or trainers still need to understand the scenario's design and purpose, its steps and the envisaged or implemented evaluation directions and possibilities.

Realism, Automation, and Open Source Ecosystems: Realism in training scenarios continues to gain importance, with many CRs now supporting complex, cyber-physical environments that include both IT and OT components. The growing need for security training in critical infrastructure sectors such as energy, transportation, healthcare, and smart cities is driving this development. Cyberattacks on train infrastructures [101], [102] or airports [103], [104], [105] highlight the emerging relevance of OT-oriented cybersecurity training also in these branches. Future research should further explore simulation fidelity and hybrid integration models, especially in the context of mobile and decentralised systems (e.g., 5G/6G-enabled networks or modular training environments). Considering the continuing integration of IT and OT, the education and training of relevant personnel is likely to become a very important branch of cybersecurity education in the future.

In parallel, automation is becoming a cornerstone of CR operations, covering infrastructure deployment, scenario execution, user simulation, and increasingly, learning evaluation. The dominance of Open Source tools such as Terraform, Ansible, and Packer points to a growing standardisation within the automation ecosystem. We expect this trend to accelerate, particularly as CRs that currently use automation to a smaller extent are likely to follow suit in the coming years, implementing and optimising automation in both their internal processes and training scenarios. A key research challenge lies in defining modular automation workflows that can be shared across platforms, thereby supporting future federated infrastructures.

Additionally, while user behaviour simulation is already common, more advanced forms such as defender simulation remain in early stages. Unlike pre-scripted users, defender agents must dynamically react to attacks in context-aware ways, requiring decision trees, knowledge graphs, and detailed system state models (e.g., OS type, installed tools, permissions). Further research is needed to develop robust frameworks for intelligent defender agents and AI-assisted simulation.

Monitoring, Evaluation, and the Role of AI: Our study also highlights a need for standardised approaches to monitoring and learning evaluation. While most CRs support some form of training assessment, tools and methods are highly heterogeneous. There is currently no broadly accepted scoring system that allows for meaningful comparison of training outcomes across platforms. Future research should therefore explore the design of interoperable evaluation frameworks and learning analytics that enable cross-platform benchmarking, certification, and integration into corporate or institutional training standards.

In this context, AI offers promising opportunities, not only for scenario generation and intelligent simulation agents, but also for multi-source data analysis during and after training. AI-based evaluation systems could help assess trainee performance, identify knowledge gaps, and provide real-time adaptive feedback or suggestions for trainees. Such developments would greatly enhance the pedagogical value of CRs and support more personalised, data-driven cybersecurity education. As mentioned earlier, automating attack and defence agents could also be an area of application.

Broadening Access and Relevance Across Sectors: Finally, there is a clear trend towards making CRs more accessible to a wider range of sectors. Although some platforms in our study have defined focus areas, the majority is not restricted to specific groups. Many offer training for multiple domains simultaneously. With increasing regulatory pressure – such as the EU NIS 2 Directive – demand for certified, scalable cybersecurity training is growing, especially in sectors like finance and banking, healthcare, space systems, but also for common organisations and companies in the private sector.

Future research should examine how CRs can be more effectively integrated into broader workforce development strategies, including certification schemes, sector-specific curricula, and alignment with national or international cybersecurity frameworks. Accredited and certified training courses for cybersecurity education must become more practical, accessible and evaluable for companies. It is therefore important that they are made comparable and thus allow to draw conclusions regarding the qualification and level of knowledge of graduates.

APPENDIX
FURTHER DETAILS ON THE CYBER RANGE SURVEY
A. DETAILS ON EXCLUDED CYBER RANGES

This section contains the CRs that were excluded during the survey as they either did not reply, did not complete the questionnaire during the survey period, did not meet our quality appraisal requirements or were not operational any more. The specific reasons why a CR platform is not part of our study can be found in the following Table 24

B. DETAILED QUESTIONNAIRE AND FLOW DIAGRAM

This section of the Appendix contains a detailed description of the questionnaire used in our survey. The questionnaire itself is composed by eight blocks, *A* to *H*, according to the categories in Section I. The questions have unique identifiers, which are printed in bold in front of the questions below.

For each block, the included questions and their answer options are outlined. The respective type of a question (e.g., open, multiple choice with closed answer options, etc.) is stated in brackets in italic directly after the question. Furthermore, there is a questionnaire flow diagram for each

TABLE 24. Cyber ranges excluded during survey.

Cyber Range	Reason for Exclusion
CITEF by Nexova / formerly RHEA	Replied positive, but did not complete the questionnaire while the survey was active
IBM/ IBM X-Force Cyber Range	Replied positive, but did not complete the questionnaire while the survey was active
Norwegian Cyber Range	Replied positive, but did not complete the questionnaire while the survey was active
Texas Cyber Range	Replied positive, but did not complete the questionnaire while the survey was active
Augusta University Cyber Range aka Georgia Cyber Range	Did not reply
Baltimore Cyber Range (BCR)	Did not reply
C4 Assessments Division of J6 of the Joint Staff (C4AD)	Did not reply
Cyber Range Hub at the Wayne State University	Did not reply
CybergymIEC	Did not reply
Cybertropolis	Did not reply
DARPA US National Cyber Range	Did not reply
DoD Cyber Range aka DoD Cyber Security Range (CSR)	Did not reply
EC-Council's CyberQ Cyber Range	Did not reply
European Space Agency (ESA) Cyber Range	Did not reply
Field Effect Cyber Range	Did not reply
Indra Cyber Range	Did not reply
INL Cyber Range	Did not reply
Joint Cyberspace Operations Range (JCOR)	Did not reply
Joint IO Range (JIOR) aka Naval Postgraduate School Cyber Range	Did not reply
Leonardo Cyber Trainer	Did not reply
ManTech Advanced Cyber Range Environment (ACRE)	Did not reply
Project Ares aka projectares.academy	Did not reply
Rochester Institute of Technology (RIT) Cyber Range	Did not reply
Try Hack Me Classrooms	Did not reply
Arizona Cyber Warfare Range	Answered that they are not interested in the purpose and goal of the survey and thus decided not to participate
Cyber Range Poulsbo	Did not participate because the platform was under major revision
CYBER RANGES / formerly Silensec Cyber Range	Answered that the management decided not to participate
CyberVAN	Decided not to participate as not developed with cybersecurity training as its sole source
Cyberdefenders Blue Yard Cyber Range	Answered that the management decided not to participate
Regent University Cyber Range	Answered that the management decided not to participate
Florida Cyber Range	Decided not to participate, without naming further reasons
DECIDE Platform	Nuari (the provider) replied that DECIDE does not have an integrated, virtualised network for defenders and is not really a Cyber Range
Cyberium	Fujitsu (the provider) answered that the project has been discontinued
Cyberwiser	Former EU project; involved persons answered that the platform is not operating any more
Michigan Cyber Range	The Merit network (the provider) answered that the platform has been discontinued
Palo Alto Cyber Range	Palo Alto (the provider) answered that the platform is not operated any more
WithSecure Playground	WithSecure (the provider) answered that the platform is not operated/sold as a product any more

block. These diagrams show the sequence of questions, but also highlight the questions or answer options that infer a conditional question sequence.

1) GENERAL QUESTIONS AND BLOCK A, DEPLOYMENT

First, block *Z* was used to query general information regarding he CR, next to the consent to participate in this study (question *Z002*):

- **Z003** – Which organization / academic institution / etc. are you affiliated with? (*open question*)
- **Z004** – What is the name of your Cyber Range product / platform? (*open question*)
- **Z005** – Have you developed the platform on your own or do you use an available Cyber Range product? (*single choice*)
  - In-house development (*closed option*)
  - We use the following available product without customizations: (*open option*)
  - We use the following available product with customizations: (*open option*)

Fig. 40 shows the sequence and dependencies of the questions in block *A*. In the following, the questions are listed. Question *A001* was used as filter for subsequent questions as can be seen from Fig. 40:

- **A001** – How is the Cyber Range deployed? (*multiple choice*)
  - On-premise (*closed option*)
  - Cloud (*closed option*)
- **A003** – Which virtualization technologies are supported? (*multiple choice*)
  - VMware (*closed option*)
  - Hyper-V (*closed option*)
  - KVM (*closed option*)
  - XenServer (*closed option*)
  - VirtualBox (*closed option*)
  - None (*closed option*)
  - Other: (*open option*)
- **A004** – Please shortly describe the type of architecture that is used in your Cyber Range: (*open question*)
- **A005** – Which cloud platforms are supported or on which platform is the Cyber Range running? (*multiple choice*)
  - Amazon AWS (*closed option*)
  - Microsoft Azure (*closed option*)
  - Google Cloud (*closed option*)
  - In-House / Private Cloud (e.g., via OpenStack or OpenNebula) (*closed option*)
  - Other: (*open option*)
- **A006 & A007** – Are container technologies used for the deployment of the Cyber Range? (*multiple choice*)
  - No container solution is used (*closed option*)
  - Yes, Docker (*closed option*)
  - Yes, Lxc (*closed option*)
  - Yes, others: (*open option*)
- **A010** – On-premise deployment: What are the hardware requirements? (*multiple choice*)
  - CPU Requirements:
    - 1 to 16 cores (*closed option*)
    - 16 to 64 cores (*closed option*)
    - 64 to 128 cores (*closed option*)
    - >128 cores (*closed option*)
  - RAM Requirements:
    - 1 to 64 GB (*closed option*)
    - 64 to 256 GB (*closed option*)
    - 256 to 1024 GB (*closed option*)

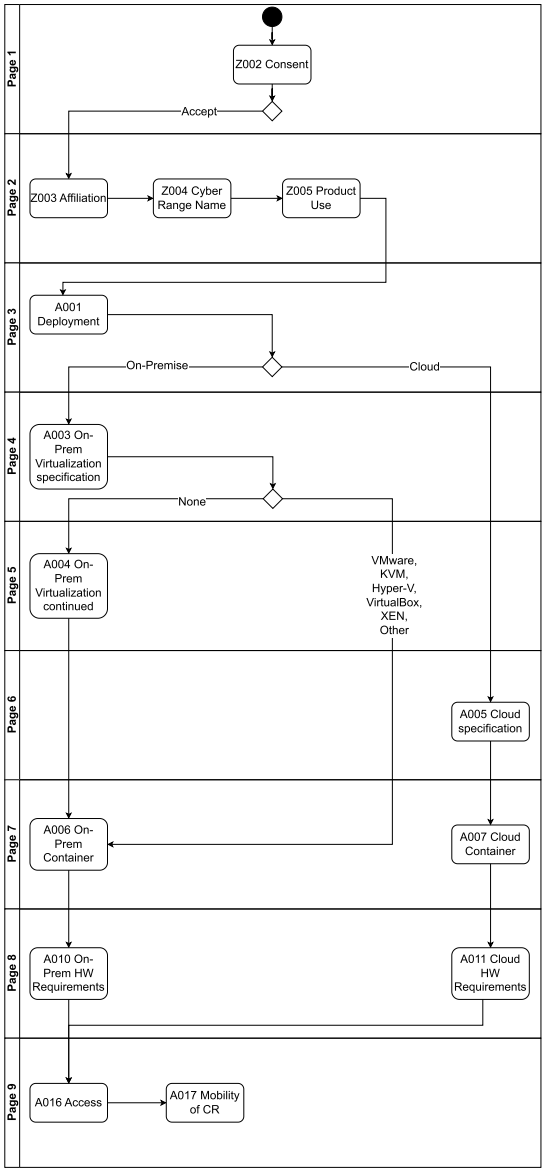


FIGURE 40. Questionnaire flow diagram Block A.

  - ∗ >1024GB (*closed option*)
- Storage Requirements:
  - ∗ up to 500 GB (*closed option*)
  - ∗ up to 2 TB (*closed option*)
  - ∗ up to 10TB (*closed option*)
  - ∗ >10TB (*closed option*)
- Need for server cluster / multiple servers:
  - ∗ Yes (*closed option*)
  - ∗ No (*closed option*)

- **A011** – Cloud deployment: What are the hardware requirements? (*multiple choice*)
  - CPU Requirements:
    - ∗ 1 to 16 cores (*closed option*)
    - ∗ 16 to 64 cores (*closed option*)
    - ∗ 64 to 128 cores (*closed option*)
    - ∗ >128 cores (*closed option*)
  - RAM Requirements:
    - ∗ 1 to 64 GB (*closed option*)
    - ∗ 64 to 256 GB (*closed option*)
    - ∗ 256 to 1024 GB (*closed option*)
    - ∗ >1024GB (*closed option*)
  - Storage Requirements:
    - ∗ up to 500 GB (*closed option*)
    - ∗ up to 2 TB (*closed option*)
    - ∗ up to 10TB (*closed option*)
    - ∗ >10TB (*closed option*)
  - Network bandwidth:
    - ∗ There is no such requirement (*closed option*)
    - ∗ 1 to 2 Gbit/s (*closed option*)
    - ∗ 2 to 10 Gbit/s (*closed option*)
    - ∗ 10 to 40 Gbit/s (*closed option*)
    - ∗ >40 Gbit/s (*closed option*)
- **A016** – In which way is the Cyber Range available to the customer? (*multiple choice*)
  - Installation on servers of the customer (*closed option*)
  - Installation in the cloud service of choice of the customer (*closed option*)
  - Shipped as an on-premise ready-to-use product (*closed option*)
  - Provided as a cloud/webplatform (*closed option*)
  - Through remote access via VPN (*closed option*)
  - In a training center of the provider (*closed option*)
  - Other: (*open option*)
- **A017** – Is the Cyber Range portable, e.g., in a mobile rack or pelican case? (*multiple choice*)
  - No portable implementation is possible (*closed option*)
  - Yes, a portable implementation is available off-the-shelf (*closed option*)
  - Yes, it can be deployed in a portable way (*closed option*)
  - Yes, it can be transported and deployed for a certain amount of time at the customer's site (e.g., contained in a truck) (*closed option*)

2) BLOCK B: QUESTIONS REGARDING PRODUCT ACCESS

Block *B* was designed to identify how the CR product can be accessed. Fig. 41 shows the sequence and dependencies of the following questions:

- **B002** – Is the Cyber Range specialized for a specific target audience? (*multiple choice*)
- **B017** – Is the Cyber Range as a product limited to certain target groups? (*multiple choice*) *B002 and B017 both with the options…*
  - No, the product is available for everyone (*closed option*)
  - Yes, to military (*closed option*)
  - Yes, to government agencies (*closed option*)

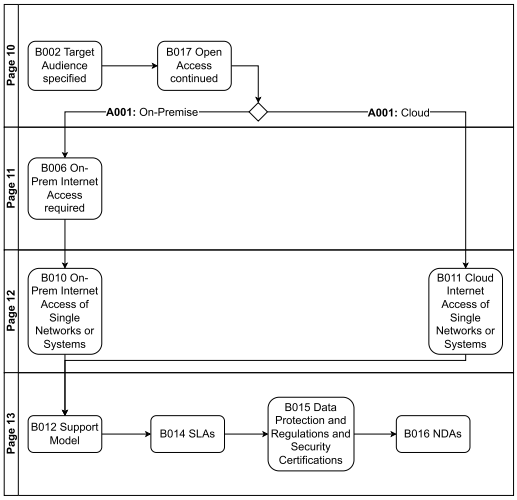


FIGURE 41. Questionnaire flow diagram Block B.

  - Yes, to critical infrastructure providers/companies (*closed option*)
  - Yes, to academia and research (*closed option*)
  - Yes, to companies (*closed option*)
  - Yes, to other: (*open option*)
- **B006** – Does the Cyber Range require Internet access? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **B010 & B011** – Does the Cyber Range allow connecting only a certain training environment, network segments or individual systems/containers, etc. within a training environment to the Internet? (*multiple choice*)
  - No, Internet is always necessary (*closed option*)
  - No, Internet is never available in training environments (*closed option*)
  - Yes, this can be configured for entire training environments (*closed option*)
  - Yes, this can be configured for specific network segments of a training environment (*closed option*)
  - Yes, this can be configured for dedicated systems within a training (*closed option*)
- **B012** – How is the maintenance of the Cyber Range handled? (*open question*)
- **B014** – Is it possible to define service level agreements? (*multiple choice*)
  - Yes, specified as follows: (*open option*)
  - No (*closed option*)
- **B015** – To which data protection regulations (e.g., the European Union's General Data Protection Regulation) and security certifications (e.g., ISO/IEC 27001) does the Cyber Range align? (*open question*)
- **B016** – Is it possible to define non-disclosure agreements? (*multiple choice*)
  - Yes (*closed option*)
  - No (*closed option*)

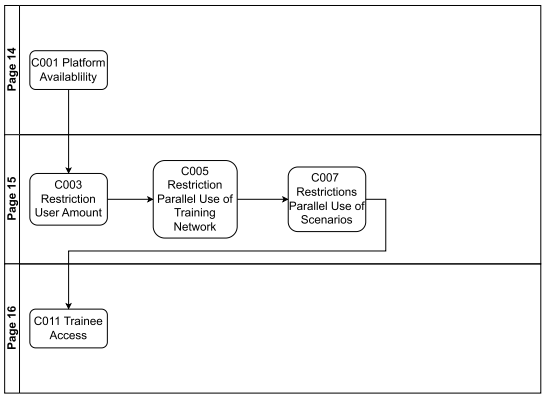


FIGURE 42. Questionnaire flow diagram Block C.

3) BLOCK C: QUESTIONS REGARDING PLATFORM ACCESS

Block *C* aimed to identify how the platform of CR product can be accessed. Its sequence is shown in Fig. 42. The respective questions were:

- **C001** – Are there restrictions in platform availability, e.g., the Cyber Range is only available during office hours? (*single choice*)
  - Yes, there are the following restrictions: (*open option*)
  - No (*closed option*)
- **C003** – Are there any restrictions, e.g., due to licensing, regarding the number of users of the Cyber Range? (*single choice*)
  - Yes, there are the following restrictions: (*open option*)
  - No (*closed option*)
- **C005** – Are there any restrictions, e.g., due to licensing, regarding the number of training environments? (*single choice*)
  - Yes, there are the following restrictions: (*open option*)
  - No (*closed option*)
- **C007** – Are there any restrictions, e.g., due to licensing, regarding the parallel use of scenarios? (*single choice*)
  - Yes, there are the following restrictions: (*open option*)
  - No (*closed option*)
- **C011** – How do trainees access the training environments? (*multiple choice*)
  - Local workstation directly connected to the training environment (*closed option*)
  - VPN (*closed option*)
  - Web browser (*closed option*)
  - Remote desktop (RDP / VNC) (*closed option*)
  - SSH (*closed option*)

4) BLOCK D: QUESTIONS REGARDING TRAINING CONTENT

Block *D* targeted the content which the CR product offers. Its sequence of questions and their conditional run-through is visualised in Fig. 43. The questions were as follows:

- **D001** – Which type of trainings are covered by the Cyber Range? (*multiple choice*)
  - Red Teaming (*closed option*)
  - Blue Teaming (*closed option*)
  - Red Team vs. Blue Team (*closed option*)
  - Red/Blue Mixed (*closed option*)
  - Capture the Flag (CTF) (*closed option*)
  - Individual Training (*closed option*)
  - Team Training (*closed option*)
  - Table-Top (*closed option*)
  - Others: (*open option*)
- **D002** – Is there a focus on a certain training type? (*single choice*)
  - There is no focus (*closed option*)
  - Yes, on Red Teaming (*closed option*)
  - Yes, on Blue Teaming (*closed option*)
  - Yes, on Red Team vs. Blue Team (*closed option*)
  - Yes, on Red/Blue Mixed (*closed option*)
  - Yes, on Capture the Flag (CTF) (*closed option*)
  - Yes, on Individual Training (*closed option*)
  - Yes, on Team Training (*closed option*)
  - Yes, on Table-Top (*closed option*)
  - Yes, on others:: (*open option*)
- **D020** – Are there officially acknowledged trainings or certifications that can be achieved? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **D021** – Which points, certificates, etc. can be awarded for a training? (*open question*)
- **D003** – Are there preconfigured scenarios available? (*multiple choice*)
  - No, there aren't (*closed option*)
  - Yes, they are bundled within the purchase of the Cyber Range product at no extra cost (*closed option*)
  - Yes, they can be purchased at additional costs (*closed option*)
  - Yes, they are community developed and shared at no extra cost (*closed option*)
  - Yes, they are community developed and included in the initial installation (*closed option*)
  - Yes, trainings with predefined scenarios are offered (*closed option*)
  - Other: (*open option*)
- **D004** – Which training categories are addressed by the preconfigured scenarios? (*multiple choice*)
  - Incident Response (IR) (*closed option*)
  - Security Operations Centre (SOC) Teaming (*closed option*)
  - Threat Hunting (*closed option*)
  - Forensics (*closed option*)
  - Critical Infrastructures (e.g., ICS/SCADA) (*closed option*)
  - Internet of Things (IoT) (*closed option*)
  - Mobile (*closed option*)
  - Network Analysis (*closed option*)
  - Malware Analysis (*closed option*)
  - Linux Analysis (*closed option*)
  - Windows Analysis (*closed option*)
  - MacOS Analysis (*closed option*)
  - Pentesting (*closed option*)
  - Malware Development (*closed option*)
  - Other (*open option*)
- **D019** – How many predefined individual training scenarios are there? (*single choice*)
- **D005** – How many predefined team training scenarios are there? (*single choice*) *D019 and D005 both with the options...*
  - There are no predefined scenarios (*closed option*)
  - 1 - 10 scenarios (*closed option*)
  - 10 - 50 scenarios (*closed option*)
  - 50 - 100 scenarios (*closed option*)
  - More than 100 scenarios (*closed option*)
- **D006** – Can existing training scenarios be customized, e.g., by changing the network structure, systems, attack path? (*single choice*)
  - Yes, as follows: (*open option*)
  - No (*closed option*)
- **D008** – Can custom scenarios be designed? (*single choice*)
  - No (*closed option*)
  - Yes, by the customer (*closed option*)
  - Yes, by the provider (*closed option*)
- **D009** – Which user roles can be trained / can participate in a training? (*multiple choice*)
  - Green Team (*closed option*)
  - White Team (*closed option*)
  - Red Team (*closed option*)
  - Blue Team (*closed option*)
  - Transparent Team (*closed option*)
  - Yellow Team (*closed option*)
  - Purple Team (*closed option*)
  - Grey Team (*closed option*)
- **D010** – Is there a feature to generate and/or inject network traffic and if yes, can it be adjusted by the user? (*single choice*)
  - Yes, it is implemented as follows: (*open option*)
  - No (*closed option*)
- **D012** – Is there a feature to simulate users and if yes can it be adjusted by the user? (*single choice*)
  - Yes, it is implemented as follows: (*open option*)
  - No (*closed option*)
- **D017** – Is there a feature to simulate defenders and if yes can it be adjusted by the user? (*single choice*)
  - Yes, it is implemented as follows: (*open option*)
  - No (*closed option*)
- **D015** – Which features to simulate attackers / attacks are used? (*multiple choice*)

  - None (*closed option*)
  - Automated live attacker systems (Kali, ParrotOS, etc.) (*closed option*)
  - Manually controlled live attacker systems (*closed option*)
  - Injects / poisoning on target systems (*closed option*)
  - Attack generator (*closed option*)
- **D016** – Please describe how the attacks in a training scenario are carried out: (*open question*)

5) BLOCK E: QUESTIONS REGARDING SUPERVISION AND SUPPORT

The level of supervision and support for training design and execution were asked in block *E*. Its conditional sequence, which depends on the output of question *D008* is presented in Fig. 44. There were the following questions:

- **E001** – Are supervised trainings offered? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **E002** – Is a train-the-trainer program offered? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **E005** – Can custom trainings be requested? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **E006** – Do you offer support for the customers when they are developing their own scenarios and trainings? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)

6) BLOCK F: QUESTIONS REGARDING INCLUDABLE PLATFORMS, SYSTEMS, AND SOFTWARE

This block queried the platforms, systems and software that are or can be included or depicted in the CR product. The sequence and dependencies of the questions are shown in Fig. 45. Questions were:

- **F012** – Which type of systems do the training environments contain? (*multiple choice*)
  - VMs (*closed option*)
  - Containers (*closed option*)
  - Hardware devices (*closed option*)
  - Other: (*open option*)
- **F001** – Which operating systems can be virtualized in the training environments? (*multiple choice*)
  - Windows (*closed option*)
  - Linux (*closed option*)
  - MacOS (*closed option*)
  - Android (*closed option*)
  - iOS (*closed option*)
  - BSD (*closed option*)

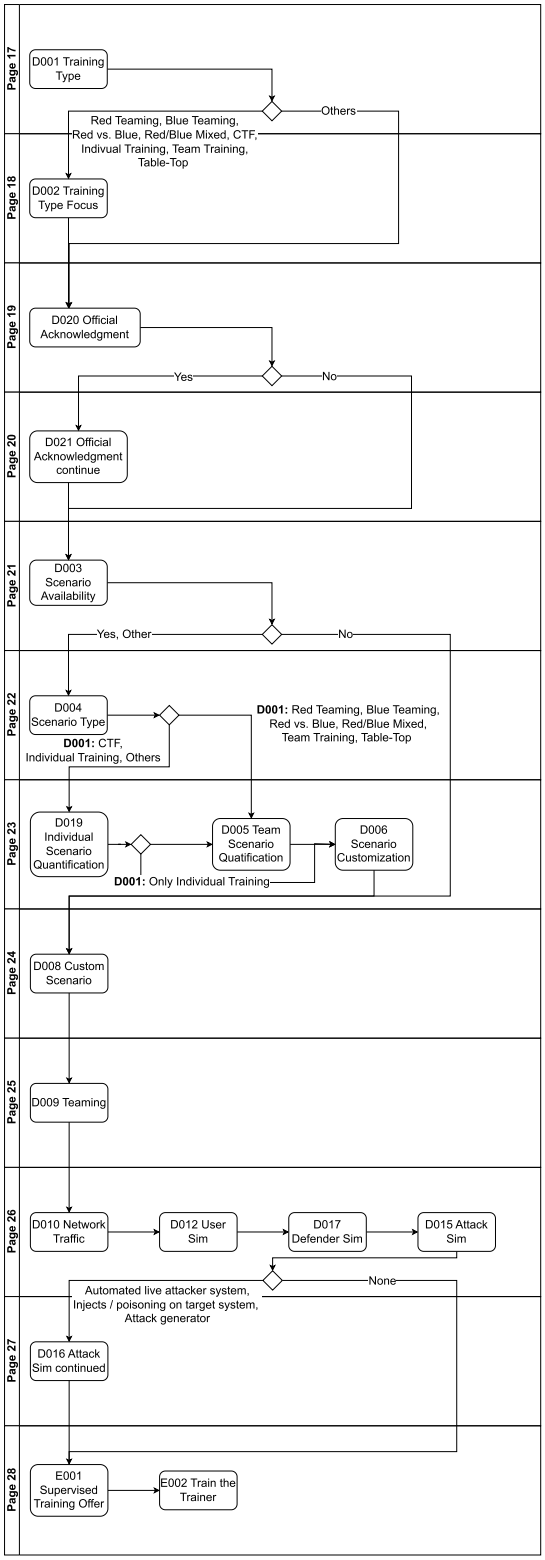


FIGURE 43. Questionnaire flow diagram block D.

  - Others: (*open option*)
- **F002 & F004** – Is it possible to integrate hardware devices in a training scenario? If yes, please specify

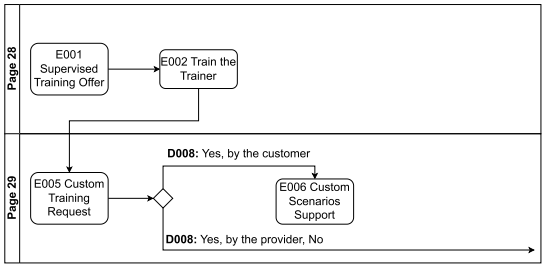


FIGURE 44. Questionnaire flow diagram block E.

and describe the used/needed interfaces (USB, Ethernet, etc.) (*single choice*)

- Yes, such devices can be attached as follows: (*open option*)
- No (*closed option*)

- **F006 & F0013** – Is there support for operational technology (OT)? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **F007 & F014** – How can the operational technology (OT) be integrated? (*single choice*)
  - Virtualised (*closed option*)
  - Physical hardware integration (*closed option*)
  - Other: (*open option*)
- **F008** – Can proprietary software or appliances (e.g., SIEM, IPS, IDS, firewalls) be included in a scenario? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **F009** – Can trainees upload and install tools or software in a training environment? (*single choice*)
  - Yes, it is implemented as follows: (*open option*)
  - No (*closed option*)
- **F015** – Is there a feature to collect memory and disk images from systems within the training environment? Can this be done either through the platform itself or manually on the systems? (*single choice*)
  - Yes, it is implemented as follows: (*open option*)
  - No (*closed option*)
- **F011** – Can client workstations of trainees (e.g., their own notebooks) be directly connected to a trainee's training environment? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)

7) BLOCK G: QUESTIONS REGARDING TRAINING EVALUATION AND LEARNING OUTCOMES

Block *G* contained four questions which aimed to cover how trainings are evaluated, and learning outcomes can be stored and evaluated. The sequence is shown in Fig. 46.

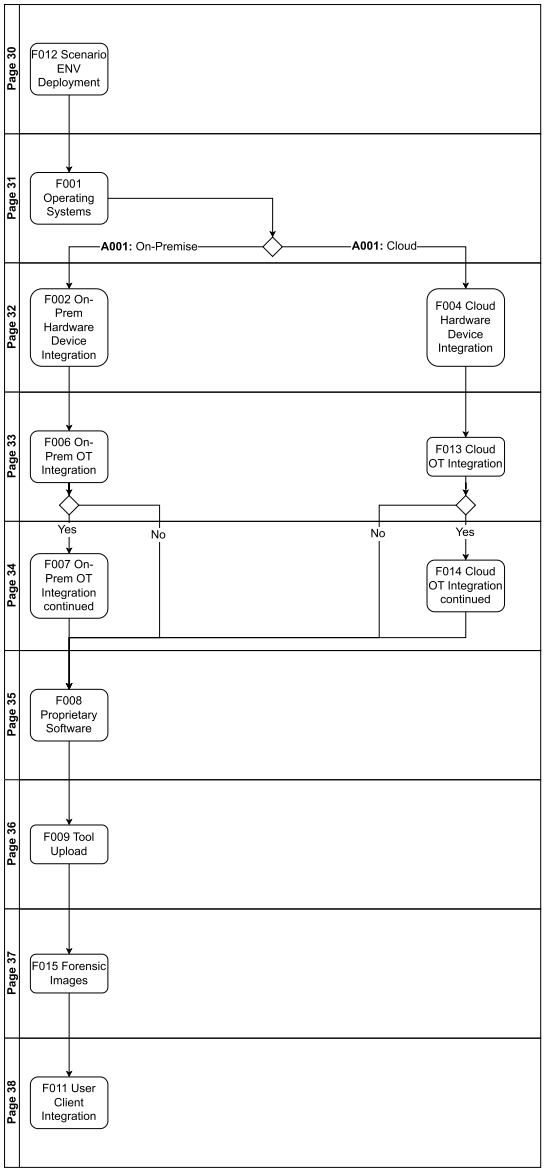


FIGURE 45. Questionnaire flow diagram block F.

- **G001** – Is a learning management system (LMS) included? (*single choice*)
  - Yes, the following LMS is included: (*open option*)
  - No (*closed option*)
- **G002** – Does the Cyber Range support the integration of LMS (other than the potentially included one)? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **G003** – Can the progress of trainees and teams be monitored? (e.g., scoring, monitoring a trainee's desktop, etc.)(*single choice*)
  - Yes, as follows: (*open option*)
  - No (*closed option*)

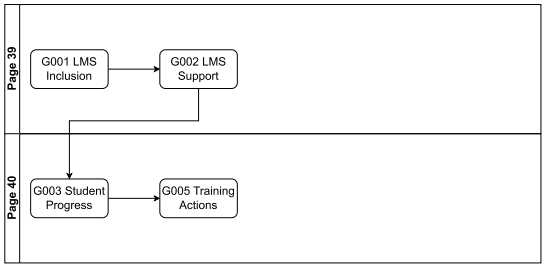


FIGURE 46. Questionnaire flow diagram block G.

- **G005** – Can the actions of trainees or teams be saved and replayed? (*single choice*)
  - No, they cannot (*closed option*)
  - Yes, the actions can be saved but not replayed (*closed option*)
  - Yes, actions can be saved and replayed (*closed option*)

8) BLOCK H: QUESTIONS REGARDING ONBOARDING, MAINTENANCE, AND CUSTOMIZATION

The final block of the questionnaire, (*H*), covered the ease of onboarding, maintenance and customisation offered by a CR. Its sequence and conditional branches are shown in the flowchart Fig. 47. The questions were as follows:

- **H001** – Is enterprise support available? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **H002** – Is there an accessible developer community /forum? (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **H003** – Does documentation on the Cyber Range software exist and is the documentation available to the customer? (*single choice*)
  - Yes, it is documented (*closed option*)
    - Documentation is accessible (*closed option*)
    - Documentation is not accessible (*closed option*)
  - No, it is not documented (*closed option*)
- **H004** – Is the scenario orchestration process documented and is the documentation available to the customer? (*single choice*)
  - Yes, it is documented (*closed option*)
    - Documentation is accessible (*closed option*)
    - Documentation is not accessible (*closed option*)
  - No, it is not documented (*closed option*)
- **H005** – Is there a set of predefined systems (e.g., a VM template library) which can be used to create or customize scenarios?(*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)
- **H006** – Can the customer design system templates to use them in training scenarios? (*single choice*)

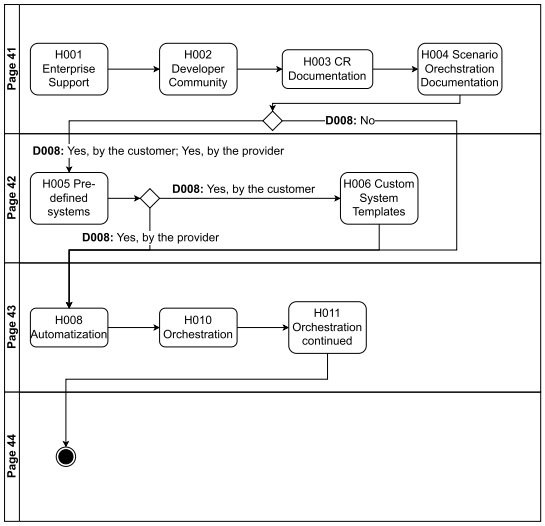


FIGURE 47. Questionnaire flow diagram block H.

  - Yes, as follows: (*open option*)
  - No (*closed option*)
- **H008** – Is automation used in order to create the training infrastructure? (e.g., training environment creation via Infrastructure as Code (IaC)) (*multiple choice*)
  - No (*closed option*)
  - Yes, by using Packer (*closed option*)
  - Yes, by using Terraform (*closed option*)
  - Yes, by using OpenTofu (*closed option*)
  - Yes, by using OpenStack Heat (*closed option*)
  - Yes, by using others: (*open option*)
- **H010** – Which orchestration software is currently used to configure a training environment? (*multiple choice*)
  - None (*closed option*)
  - Ansible (*closed option*)
  - Puppet (*closed option*)
  - Chef (*closed option*)
  - VMware Aria Automation Orchestrator (formerly vRealize Orchestrator) (*closed option*)
  - Microsoft System Center Orchestrator (SCOrch) (*closed option*)
  - Other (*open option*)
- **H011** – Does the Cyber Range enable the usage of open orchestration software? (e.g., Ansible, Puppet) (*single choice*)
  - Yes (*closed option*)
  - No (*closed option*)

REFERENCES

[1] (Dec. 2023). *Boardroom Cybersecurity 2023 Report*. [Online]. Available: https://www.secureworks.com/resources/rp-boardroom-cybersecurity-report-2023
[2] (Jul. 2023). *Cost of a Data Breach Report 2023*. [Online]. Available: https://www.ibm.com/reports/data-breach
[3] Federal Office for Information Security. (Nov. 2023). *Die Lage Der IT-Sicherheit in Deutschland 2023*. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

[4] IBM. (Feb. 2023). *Threat Intelligence Index 2023*. [Online]. Available: https://www.ibm.com/downloads/cas/DB4GL8YM

[5] (May 2019). *2019 Data Breach Investigations Report*. [Online]. Available: https://www.verizon.com/business/resources/reports/2019/2019-data-breach-investigations-report.pdf

[6] M. Knüpfer, T. Bierwirth, L. Stiemert, M. Schopp, S. Seeber, D. Pöhn, and P. Hillmann, "Cyber taxi: A taxonomy of interactive cyber training and education systems," in *Model-driven Simulation and Training Environments for Cybersecurity*. Cham, Switzerland: Springer, 2020, pp. 3–21. [Online]. Available: https://link.springer.com/10.1007/978-3-030-62433-0_1

[7] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101636. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404819301804

[8] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds," Defence Science and Technology Organisation, Edinburgh, Scotland, Tech. Rep. DSTO-GD-0771, Oct. 2013. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA594524.pdf

[9] S. Leblanc, A. Partington, I. M. Chapman, and M. Bernier, "An overview of cyber attack and computer network operations simulation," in *Proc. Mil. Model. Simul. Symp.*, 2011, pp. 92–100.

[10] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, "A review of cyber-ranges and test-beds: Current and future trends," *Sensors*, vol. 20, no. 24, p. 7148, Dec. 2020.

[11] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and TestBeds for education, training, and research," *Appl. Sci.*, vol. 11, no. 4, p. 1809, Feb. 2021.

[12] S. Steiner, A. Jillepalli, and D. C. de Leon, "A survey of cloud-hosted, publicly-available cyber-ranges for educational institutions," *J. Comput. Sci. Colleges*, vol. 38, no. 1, pp. 68–77, 2022.

[13] W. Lazarov, T. Stodulka, T. Schafeitel-Tähtinen, M. Helenius, and Z. Martinasek, "Interactive environment for effective cybersecurity teaching and learning," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–9.

[14] P. Jani, S. Karo, S. Jarno, S. Tuomo, V. Jan, and K. Tero, "Cyber range: Preparing for crisis or something just for technical people?" in *Proc. 20th Eur. Conf. Cyber Warfare Secur.*, 2021, pp. 1–16.

[15] ECSO. (Jan. 2024). *GBCyber Range Features Checklist & List of European Providers: Updated 2024 Edition*. [Online]. Available: https://ecs-org.eu/cyber-range-features-checklist-list-of-european-providers-updated-2024-edition/

[16] *European Cyber Security Organisation*. Accessed: Jan. 28, 2024. [Online]. Available: https://ecs-org.eu/

[17] National initiative for cybersecurity education (NICE). (Sep. 2023). *The Cyber Range: A Guide*. [Online]. Available: https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

[18] *General Data Protection Regulation (GDPR) Compliance Guidelines*. Accessed: Feb. 9, 2024. [Online]. Available: https://gdpr.eu/

[19] *ISO/IEC 27001:2022*. Accessed: Feb. 9, 2024. [Online]. Available: https://www.iso.org/standard/27001

[20] R. Uetz, C. Hemminghaus, L. Hackländer, P. Schlipper, and M. Henze, "Reproducible and adaptable log data generation for sound cybersecurity experiments," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2021, pp. 690–705.

[21] Y. Geng, Y. Wang, W. Liu, Q. Wei, K. Liu, and H. Wu, "A survey of industrial control system testbeds," in *Proc. 20th Nordic Conf. Secure IT Syst.*, vol. 569, Stockholm, Sweden, Oct. 2019, pp. 11–26.

[22] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," *SSRN Electron. J.*, vol. 37, no. 43, pp. 879–910, Nov. 2015.

[23] R. B. Briner and D. Denyer, "Systematic review and evidence synthesis as a practice and scholarship tool," in *The Oxford Handbook of Evidence-Based Management*, D. M. Rousseau, Ed., London, U.K.: Oxford Univ. Press, 2012, pp. 112–129, doi: 10.1093/oxfordhb/9780199763986.013.0007.

[24] A. Fink, *Conducting Research Literature Reviews: From the Internet to Paper*. Newbury Park, CA, USA: Sage, Jan. 2019.

[25] CONCORDIA consortium. *Cyber Security Competence for Research and Innovation (CONCORDIA)*. Accessed: Jan. 28, 2024. [Online]. Available: https://www.concordia-h2020.eu/

[26] R. Beuran, J. Vykopal, D. Belajová, P. Celeda, Y. Tan, and Y. Shinoda, "Capability assessment methodology and comparative analysis of cybersecurity training platforms," *Comput. Secur.*, vol. 128, May 2023, Art. no. 103120. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823000305

[27] S. R. Chowdhury, M. A. Oakkas, and F. Ahmmed, "Survey questionnaire," in *Principles of Social Research Methodology*, M. R. Islam, N. A. Khan, and R. Baikady, Eds., Cham, Switzerland: Springer, 2022, pp. 181–205.

[28] L. A. Ritter and V. M. Sue, "The survey questionnaire," *New Directions Eval.*, vol. 2007, no. 115, pp. 37–45, 2007. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ev.234

[29] J. A. Krosnick, "Questionnaire design," in *The Palgrave Handbook of Survey Research*, D. L. Vannette and J. A. Krosnick, Eds., Cham, Switzerland: Springer, 2017, pp. 439–455. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-54395-6_53

[30] *SoSci Survey–die Lösung Für Professionelle Onlinebefragung*. Accessed: Jan. 7, 2025. [Online]. Available: https://www.soscisurvey.de/

[31] *Virtualization Platform–Overview*. Accessed: Feb. 4, 2025. [Online]. Available: https://6sense.com/tech/virtualization

[32] P. Sharma, L. Chaufournier, P. Shenoy, and Y. C. Tay, "Containers and virtual machines at scale: A comparative study," in *Proc. 17th Int. Middleware Conf.*, Nov. 2016, pp. 1–13.

[33] R. K. Ellis, "Learning management systems," Amer. Soc. Training Develop. (ASTD), Alexandria, VA, USA, Tech. Rep., 2009.

[34] D. Jacquette, *Ontology*. Evanston, IL, USA: Routledge, 2014.

[35] *DECIDE: Cyber Security Live Exercises*. Accessed: May 28, 2024. [Online]. Available: https://nuari.org/decide

[36] M. Leitner, M. Frank, W. Hotwagner, G. Langner, O. Maurhart, T. Pahi, L. Reuter, F. Skopik, P. Smith, and M. Warum, "AIT cyber range: Flexible cyber security environment for exercises, training and research," in *Proc. Eur. Interdiscipl. Cybersecurity Conf.*, Nov. 2020, pp. 1–6.

[37] E. Moore, S. Fulton, R. A. Mancuso, T. K. Amador, and D. Likarish, "A layered model for building cyber defense training capacity," in *Proc. IFIP World Conf. Inf. Secur. Educ.*, 2021, pp. 64–80.

[38] T. Gustafsson and J. Almroth, "Cyber range automation overview with a case study of CRATE," in *Proc. Nordic Conf. Secure IT Syst.*, 2021, pp. 192–209.

[39] A. Grigoriadis, E. Darra, D. Kavallieros, E. Chaskos, N. Kolokotronis, and X. Bellekens, "Cyber ranges: The new training era in the cybersecurity and digital forensics world," in *Technology Development for Security Practitioners*. Cham, Switzerland: Springer, 2021, pp. 97–117.

[40] F. Frati, G. Darau, N. Salamanos, P. Leonidou, C. Iordanou, D. Plachouris, E. Syrmas, E. Floros, G. Nikitakis, G. Spanoudakis, K. Kalais, S. Tsichlaki, E. Damiani, G. C. Kagadis, J. Najar, and M. Sirivianos, "Cybersecurity training and healthcare: The AERAS approach," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1527–1539, Apr. 2024.

[41] I. Bica, R. L. Unc, and Ş. Ţurcanu, "Virtualization and automation for cybersecurity training and experimentation," in *Proc. Int. Conf. Inf. Technol. Commun. Secur.*, 2021, pp. 227–241.

[42] M. Puys, P.-H. Thevenon, and S. Mocanu, "Hardware-in-the-loop labs for SCADA cybersecurity awareness and training," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–10.

[43] A. Bécue, M. Praddaude, E. Maia, N. Hogrel, I. Praça, and R. Yaich, "Digital twins for enhanced resilience: Aerospace manufacturing scenario," in *Proc. Int. Conf. Adv. Inf. Syst. Eng.* Cham, Switzerland: Springer, 2022, pp. 107–118.

[44] A. Grimaldi, J. Ribiollet, P. Nespoli, and J. Garcia-Alfaro, "Toward next-generation cyber range: A comparative study of training platforms," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2023, pp. 271–290.

[45] E. Maia, D. Lancelin, J. Carneiro, T. Oudin, Á. Dória, and I. Praça, "Intelligent cyberattack detection on safecare virtual hospital," in *Proc. World Conf. Inf. Syst. Technol.* Cham, Switzerland: Springer, 2022, pp. 327–337.

[46] T. Lieskovan, D. Kohout, and J. Frolka, "Cyber range scenario for smart grid security training," *e+i Elektrotechnik und Informationstechnik*, vol. 140, no. 5, pp. 452–459, 2023.

[47] J. Almroth and T. Gustafsson, "CRATE exercise control—A cyber defense exercise management and support tool," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Sep. 2020, pp. 37–45.

[48] B. Liu, A. Cheng, and Y. Zhou, "A review of cyberspace operations modeling and simulation research and suggestions," in *Proc. Asian Simul. Conf.*, 2022, pp. 491–502.
[49] J. Zhang, Z. Li, R. Chen, W. Han, N. Hu, and Y. Zhang, "A survey of cyber range: Current status, analysis, and future trends," in *Proc. Int. Conf. Netw. Simul. Eval.*, 2024, pp. 88–101.
[50] T. Sommestad and U. Franke, "A test of intrusion alert filtering based on network information," *Secur. Commun. Netw.*, vol. 8, no. 13, pp. 2291–2301, Sep. 2015.
[51] M. Välja, F. Heiding, U. Franke, and R. Lagerström, "Automating threat modeling using an ontology framework," *Cybersecurity*, vol. 3, no. 1, pp. 1–20, Dec. 2020.
[52] M. Almgren, P. Andersson, G. Björkman, M. Ekstedt, J. Hallberg, S. Nadjm-Tehrani, and E. Westring, "RICS-El: Building a national testbed for research and training on SCADA security (Short paper)," in *Proc. Int. Conf. Crit. Inf. Infrastructures Secur.* Cham, Switzerland: Springer, 2018, pp. 219–225.
[53] *Thales Cyber Range Powered By Diateam*. Accessed: Mar. 1, 2025. [Online]. Available: https://www.thalesgroup.com/en/cyber-range-powered-diateam
[54] *Immerisve Labs*. Accessed: Oct. 9, 2024. [Online]. Available: https://www.immersivelabs.com/
[55] G. Hatzivasilis et al., "The THREAT-ARREST cyber range platform," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2021, pp. 422–427.
[56] N. Miloslavskaya and A. Tolstoy, "Cyber polygon site project in the framework of the MEPhI network security intelligence center," in *Proc. 11th Annu. Meeting Brain-Inspired Cogn. Archit. Artif. Intell.* Cham, Switzerland: Springer, 2020, pp. 295–308.
[57] T. Balon and I. Baggili, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," *Educ. Inf. Technol.*, vol. 28, no. 9, pp. 11759–11791, Sep. 2023.
[58] M. Andreolini, V. G. Colacino, M. Colajanni, and M. Marchetti, "A framework for the evaluation of trainee performance in cyber range exercises," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 236–247, Feb. 2020.
[59] P. D. L. Vallée, G. Iosifidis, A. Rossi, M. Dri, and W. Mees, "Sector-specific training–A federated maritime scenario," in *Proc. Int. Conf. Multimedia Commun.*, 2022, pp. 21–35.
[60] R. Beuran, D. Tang, C. Pham, K.-I. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: Cytrone," *Comput. Secur.*, vol. 78, pp. 43–59, Sep. 2018.
[61] R. Beuran, Z. Zhang, and Y. Tan, "AWS EC2 public cloud cyber range deployment," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Jun. 2022, pp. 433–441.
[62] G. Vigna, "Teaching hands-on network security: Testbeds and live exercises," *J. Inf. Warfare*, vol. 2, no. 3, pp. 8–24, 2003.
[63] J.-M. Su, "WebHOLE: Developing a Web-based hands-on learning environment to assist beginners in learning Web application security," *Educ. Inf. Technol.*, vol. 29, no. 6, pp. 6579–6610, Apr. 2024.
[64] H. Feng and Y. Li, "Deliberated vulnerable environment generating based on container and structured vulnerability intelligence," in *Proc. Int. Conf. Artif. Intell. Secur.*, 2020, pp. 549–557.
[65] B. Nikolov, "Improving cybersecurity capabilities at Nikola vaptsarov naval academy by building and developing a security operations and training center," in *Proc. Int. Conf. Digit. Transformation*, 2023, pp. 219–242.
[66] Research Institute CODE. *Cyber Range ICE&T*. Accessed: Feb. 3, 2025. [Online]. Available: https://www.unibw.de/code/forschung/zentrallabore/cyber-range
[67] S. Shrivastava, F. Furtado, M. Goh, and A. Mathur, "The design of cyber-physical exercises (CPXS)," in *Proc. 14th Int. Conf. Cyber Conflict: Keep Moving! (CyCon)*, vol. 700, May 2022, pp. 348–366.
[68] *Laokoon Security–Cyber Ranges*. Accessed: Feb. 9, 2025. [Online]. Available: https://laokoon-security.com/en/service/cyber-ranges/
[69] *Luxembourg Cyber Range*. Accessed: Feb. 9, 2025. [Online]. Available: https://cyber-range.lu/
[70] K. B. Vekaria, P. Calyam, S. Wang, R. Payyavula, M. Rockey, and N. Ahmed, "Cyber range for research-inspired learning of 'attack defense by pretense' principle and practice," *IEEE Trans. Learn. Technol.*, vol. 14, no. 3, pp. 322–337, Mar. 2021.
[71] X. Wei, C. Lu, F. R. Ozcan, T. Chen, B. Wang, D. Wu, and Q. Tang, "A behavior-aware profiling of smart contracts," in *Proc. 15th EAI Int. Conf. Secur. Privacy Commun. Netw.*, Orlando, FL, USA. Cham, Switzerland: Springer, Oct. 2019, pp. 245–258.
[72] D. Ionică, N. Popescu, D. Popescu, and F. Pop, "Cyber defence capabilities in complex networks," in *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*. Cham, Switzerland: Springer, 2018, pp. 217–231.
[73] S. Puuska, T. Kokkonen, J. Alatalo, and E. Heilimo, "Anomaly-based network intrusion detection using wavelets and adversarial autoencoders," in *Proc. 11th Int. Conf. Innov. Secur. Solutions Inf. Technol. Commun.*, Bucharest, Romania. Cham, Switzerland: Springer, 2019, pp. 234–246.
[74] M. Masdari and H. Khezri, "Towards fuzzy anomaly detection-based security: A comprehensive review," *Fuzzy Optim. Decis. Making*, vol. 20, no. 1, pp. 1–49, Mar. 2021.
[75] K. Olejnik, M. Atighetchi, and S. Blais, "The semantic processing pipeline: Quantifying the network-wide impact of security tools," in *Proc. Workshop Dyn. Novel Adv. Mach. Learn. Intell. Cyber Secur.*, Dec. 2020, pp. 1–8.
[76] J. M. Couretas, "Cyber modeling & simulation (M&S) for test and evaluation (T&E)," in *An Introduction to Cyber Modeling and Simulation*. Hoboken, NJ, USA: Wiley, 2019, pp. 125–136.
[77] J. M. Couretas, "Cyber modeling and simulation for analysis and targeting," in *An Introduction to Cyber Analysis and Targeting*. Cham, Switzerland: Springer, 2022, pp. 221–247.
[78] X. Larrucea and I. Santamaría, "Designing a cyber range exercise for educational purposes," in *Proc. 27th Eur. Conf. Softw. Services Process Improvement*, Düsseldorf, Germany. Cham, Switzerland: Springer, 2020, pp. 302–312.
[79] A. Peratikou, C. Louca, S. Shiaeles, and S. Stavrou, "On federated cyber range network interconnection," in *Proc. 12th Int. Netw. Conf. Sel. Papers*, 2021, pp. 117–128.
[80] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[81] O. Darwish, C. M. Stone, O. Karajeh, and B. Alsinglawi, "Survey of educational cyber ranges," in *Proc. Workshops 34th Int. Conf. Adv. Inf. Netw. Appl. Web, Artif. Intell. Netw. Appl.* Cham, Switzerland: Springer, 2020, pp. 1037–1045.
[82] *CRATE–Sweden's National Cyber Training Facility*. Accessed: Sep. 24, 2024. [Online]. Available: https://www.foi.se/en/foi/research/information-security/crate—swedens-national-cyber-training-facility.html
[83] *Forschungsinstitut CODE–Über Uns*. Accessed: Sep. 20, 2024. [Online]. Available: https://www.unibw.de/code/im-profil/ziele
[84] *UNSW Canberra–About Us*. Accessed: Oct. 4, 2024. [Online]. Available: https://www.unsw.edu.au/canberra/about-us
[85] The OpenStack project. (2025). *The Most Widely Deployed Open Source Cloud Software in the World*. [Online]. Available: https://www.openstack.org/
[86] *Openstack Documentation–Feature Classification*. Accessed: Oct. 26, 2024. [Online]. Available: https://docs.openstack.org/nova/latest/user/feature-classification.html
[87] (2025). *Proxmox Virtual Environment*. [Online]. Available: https://www.proxmox.com/en/proxmox-virtual-environment/overview
[88] F. Bellard. (2020). *Qemu–Main Page*. [Online]. Available: https://wiki.qemu.org/MainPage
[89] Galaxy Technologies LLC. (2024). *Getting Started With GNS3*. [Online]. Available: https://docs.gns3.com/docs/
[90] The Kubernetes Authors. (2024). *Kubernetes Features*. [Online]. Available: https://kubernetes.io/
[91] Keystone Education Group. (2024). *What Are Ceus?*. [Online]. Available: https://www.findcourses.com/prof-dev/what-is-ceu-9413
[92] (2024). *Unlock the Power of Your People*. [Online]. Available: https://info.credly.com/
[93] Progress Software Corporation. (2024). *Cloud-Powered Job Orchestration is Here*. [Online]. Available: https://www.chef.io/
[94] (2024). *Automate Infrastructure on Any Cloud With Terraform*. [Online]. Available: https://www.terraform.io/
[95] (2024). *The Open Source Infrastructure As Code Tool*. [Online]. Available: https://opentofu.org/
[96] (2024). *Automate Image Builds With Packer*. [Online]. Available: https://www.packer.io/
[97] The OpenStack project. (2024). *Heat–Openstack Orchestration*. [Online]. Available: https://wiki.openstack.org/wiki/Heat
[98] I. Lates and C. Boja, "Cyber range technology stack review," in *Proc. 21st Int. Conf. Informat. Economy Educ., Res. Bus. Technol.* Cham, Switzerland: Springer, 2023, pp. 25–40.

[99] European Defence Agency. (2021). *Cyber Ranges Federation Project*. [Online]. Available: https://eda.europa.eu/docs/default-source/eda-factsheets/2021-07-05-factsheet-cyber-ranges.pdf
[100] ECHO Network. (2024). *Project Summary–ECHO Network*. [Online]. Available: https://echonetwork.eu/project-summary/
[101] J. Thurau. *Germany's Critical Infrastructure is Poorly Protected*. Accessed: Apr. 20, 2025. [Online]. Available: https://www.dw.com/en/germanys-critical-infrastructure-is-poorly-protected/a-63505983
[102] (2024). *Cyber-Attacks Received in the Railway Sector*. [Online]. Available: https://phoeni2x.eu/2024/02/29/cyber-attacks-received-in-the-railway-sector/
[103] H. McDonald. (2024). *Major Cyber Attack Disrupts Holiday Season Flights at Japan Airlines*. [Online]. Available: https://www.euronews.com/business/2024/12/26/major-cyber-attack-disrupts-holiday-season-flights-at-japan-airlines
[104] C. Kunz. *Cyber Attack on German Air Traffic Control–is APT28 Behind It?*. Accessed: Apr. 19, 2025. [Online]. Available: https://www.heise.de/en/news/Cyber-attack-on-German-air-traffic-control-is-APT28-behind-it-9853990.html
[105] F. Nizam. (2025). *Cyberattack on MAHB: Hackers Yet To Be Identified*. [Online]. Available: https://www.nst.com.my/news/nation/2025/03/1193233/cyberattack-mahb-hackers-yet-be-identified

CHRISTOPH STEININGER received the B.Sc. and M.Sc. degrees in business computing from The University of Passau, Germany, in 2017 and 2020, respectively, and the M.Sc. degree in global information technology management from the University of Turku, Finland, in 2020.

He is currently a Research Assistant and a Ph.D. Student with the Research Institute CODE, University of the Bundeswehr Munich, Germany. He holds the cybersecurity certifications OSCP and OSWP and is involved in conducting cyber range training in the Cyber Range ICE&T, Research Institute CODE. His research interests include system security with a focus on cybersecurity and cyber range training, attacker methodology, and cyber range architectures.

LAURA GÖTZ received the B.A. degree in media informatics from the University of Regensburg, Germany, in 2018, and the M.Sc. degree in human–computer interaction from LMU Munich, Germany, in 2021.

She is currently a Research Assistant with the Research Institute CODE, University of the Bundeswehr Munich, Germany. Her research interests include the conception, development, and analysis of cybersecurity training, with a focus on effective team composition, participant performance evaluation, and the design of a continuous feedback process.

MATTHIAS SCHOPP received the B.Sc. degree in business computer science from Baden-Württemberg Cooperative State University and the B.A. degree in business administration from the Open University Milton Keynes, in 2011, and the M.Sc. degree in computer science from the Ludwig-Maximilians-University of Munich, Germany, in 2014.

He is currently the Laboratory Supervisor of the Cyber Range ICE&T, Research Institute CODE, University of the Bundeswehr Munich, Germany, with the main tasks of developing new cybersecurity scenarios and implementing and executing cyber range training. His research interests include system security with a focus on cybersecurity and cyber range training, attacker methodology, and cyber range architectures.