International Journal of Information Security (2026) 25:140
https://doi.org/10.1007/s10207-026-01298-y

REGULAR CONTRIBUTION

Engineering cyber ranges and security testbeds: a survey of technologies, use cases, and research trends

Klaus Mayer[1] · Max Landauer[1] · Florian Skopik[1] · Markus Wurzenberger[1]

Received: 9 March 2026 / Accepted: 25 June 2026 / Published online: 10 August 2026
© The Author(s) 2026

Abstract

This survey examines how cyber ranges (CRs) and testbeds (TBs) are implemented in practice by focusing on the technologies used to realise CR/TB use cases and features. Building on a systematic literature review spanning 2020–Aug. 2025, the study includes 199 publications and consolidates extracted application areas, purposes, use cases, infrastructure types, and reported technologies into a structured data repository for analysis. The repository identifies 650 distinct technologies and maps them into a hierarchical structure of 10 technology domains and 81 technology subdomains to support consistent cross-paper comparison despite heterogeneous terminology and architectural representations. The analysis indicates a functional separation in reported deployments, with TBs reported more frequently for experimentation-oriented use cases, whereas CRs are reported more frequently for training, exercises, and education. Across application areas, the data show concentrated profiles and explicit domain/application-area gaps where no technologies are reported for specific combinations, and temporal trends indicate increasing diversification of reported use cases in 2024–2025. Based on these patterns and the discussed challenges of inconsistent terminology and categorization, the paper recommends more systematic reporting of technologies and feature implementations and the use of shared terminology with explicit mappings to reference architectures or taxonomies.

Keywords Cyber ranges · Testbeds · Cyber security training · Cyber security education · Cyber attack scenarios · Red teaming · Computing platform

1 Introduction

Cyber ranges (CRs) and testbeds (TBs) are essential in modern cybersecurity. They provide realistic platforms for training professionals in the field of information and communication technology (ICT), which becomes increasingly important given the rising number of cyberattacks and threats. The importance and relevance of CRs and TBs in cybersecurity is steadily increasing and has been emphasized repeatedly in related surveys published in recent years [189]. In addition, their versatile scientific use for research, experimentation and testing [91], as well as their adoption in industry, further confirms the relevance of these technologies [71]. According to [71], there remains a need for clear guidelines covering the conception, development, evaluation, and operation of CRs. While several studies address key aspects of CRs, they often primarily reiterate or paraphrase established standards, and in some cases interpret them inconsistently, rather than offering additional novel insights and concrete, unambiguous guidance for designing and operating a CR. As also noted in [189], despite their growing relevance, research gaps persist and a comprehensive, consolidated analysis serving as a central reference for the community is still missing.

A key challenge in designing and operating a CR or a TB is the large number of potentially suitable technologies and the resulting complexity of technology selection. For example, during our literature analysis, we identified 650 distinct technologies that can be used to develop CRs, TBs, and different use cases. This motivated the following research questions:

✉ Klaus Mayer
klaus.mayer@ait.ac.at

Max Landauer
max.landauer@ait.ac.at

Florian Skopik
florian.skopik@ait.ac.at

Markus Wurzenberger
markus.wurzenberger@ait.ac.at

[1] Austrian Institute of Technology, Vienna, Austria

- RQ1: What use cases and application areas for cyber ranges (CRs) and testbeds (TBs) are reported in the literature?
- RQ2: Which technologies and technology groups are used to implement specific CR/TB features?
- RQ3: What trends and notable patterns can be observed in the research and development of cyber ranges and testbeds (e.g., purposes, application areas, and technologies)?

A substantial share of existing surveys focuses on general features and the architecture of CRs and TBs. Several approaches propose taxonomies and models to categorize features and functions, use cases, and architectural representations. However, to the best of the authors' knowledge, the only survey that primarily focuses on the digital building blocks of a CR or TB, specifically the technologies used to implement them, is [208]. Therefore, the goal of this work is to provide an overview of current technologies and to facilitate the selection of technologies for implementing use cases and features in CRs and TBs. As a starting point, we build on [208], which provides a list of technologies, including the documented year and domain of application, that have been used in CRs and TBs. In summary, this paper makes the following contributions:

- An overview of CRs and TBs, including their *application areas* and purposes.
- A list of technologies used in CRs and TBs, together with their intended use.
- The identification of gaps and notable patterns regarding technologies, CRs, and TBs.

2 Background and related work

This section summarizes relevant publications that address cyber range (CR) and testbed (TB) functionalities, capabilities, and architectural aspects. The key contributions extracted from these works include classifications and taxonomies of CR/TB characteristics, proposed reference architectures, frameworks, or conceptual models, and evaluations of existing CRs/TBs, including discussions of *purposes*, *application areas*, and supporting technologies.

Ukwandu et al. [189] provide a systematic overview of CRs and security TBs, focusing on how these platforms are used for cybersecurity training and how they could evolve in light of increasing attack automation and the convergence of information technology (IT) and operational technology (OT). They examine literature mainly from 2015 to 2020 and analyse CR/TB platforms by *application areas*, deployment model, experimentation approach (simulation, emulation, hybrid), team structures, and underlying technologies such as virtualization, containerization, and physical hardware. Based on this synthesis, the article compares typical scenario characteristics and attack types in CRs and TBs. It finds that TBs are often linked to critical infrastructures and OT environments, whereas CRs are more commonly used in ICT-oriented education and training. A key contribution of the article is the proposal of two dedicated taxonomies. One taxonomy focuses on CRs, and the other focuses on TBs. These taxonomies organise aspects such as management and monitoring, scenario design (which includes educational mechanisms and gamification), attack types, and recovery-related features. The taxonomy for TBs also includes additional dimensions for modelling and execution. The authors also discuss the training methods supported by CRs and TBs. They argue that the distinction between these two platform types is becoming less clear. The article highlights emerging trends, including the development of more configurable and real-time environments, as well as broader application contexts such as cyber-physical systems and Industry 4.0. Potential enhancements, such as the integration of augmented reality, are also explored.

Chouliaras et al. [38] review cyber ranges and security testbeds used for cybersecurity education, training, exercises, and research, addressing the practical gap that many studies mention platforms but give limited detail on architecture, topology, and concrete implementation tools. The authors first compile and characterise a set of cyber ranges/testbeds from the literature (e.g., by operator, objectives, sector, environment type, and infrastructure), and then conduct structured interviews with technical directors/managers of ten selected platforms to capture otherwise underreported design and operational details, including scenario creation and deployment, exercise management, and the technologies used. Based on the interview data, the paper synthesises a tool- and component-oriented view of contemporary cyber range implementations. It reports common usage patterns (primarily training, often combined with research/exercises), covered domains such as competitions and SCADA/ICS, and typical challenge areas (e.g., web security, forensics, exploitation, and malware analysis). The study also documents frequently used technology choices across platforms, including cloud and infrastructure solutions (e.g., OpenStack and AWS), virtualization and container approaches (e.g., hypervisors and Docker), IaC tooling (e.g., Ansible, Vagrant, and Packer), scenario-description formats (mainly JSON and YAML), and monitoring/security components (e.g., OSSIM, Nagios, Snort, and Suricata), and discusses dataset generation, remote access/federation, and a trend toward digital-twin-like environments.

Kampourakis et al. [71] propose a fine-grained reference architecture for cyber ranges, motivated by IT/OT convergence in Industry 5.0 and the need for realistic, standards-aligned environments for cybersecurity preparedness. They

argue that existing work does not jointly address cyber range design, development, evaluation, and operation in a complete and up-to-date manner. To close this gap, the authors derive an abstract model from relevant guidelines and standards, refine it using commonly reported cyber range functionalities and traits, and introduce an evaluation formula to estimate how closely a given cyber range aligns with the state of the art. The main contribution is an architecture description that is structured according to ISO/IEC/IEEE 42010. It is organised into structural, functional, and informational views.In the structural view, the targeted environment can be either a dedicated testbed or a digital twin. This environment is embedded within layers responsible for infrastructure, virtualization, and orchestration. The paper examines typical virtualization options, which include public or private cloud solutions, virtual machines, and containers. It also references platforms such as AWS, OpenStack, VMware, and Docker. Additionally, the paper addresses orchestration methods, including the use of controllers, Infrastructure as Code (IaC), and APIs. The evaluation method is demonstrated through example assessments using criterion-based scoring and visual comparison, and the authors position the work as a basis for improved unification and standardization, with a proof-of-concept implementation planned as future work.

Collectively, the aforementioned works provide a systematic overview of CRs, primarily focusing on architectures, taxonomies, and the structural and functional concepts underlying CR design. Yamin et al. [208] present a systematic literature review of unclassified CRs and security TBs as environments for executing cybersecurity training scenarios, covering both skill-oriented training for security professionals and broader awareness-focused training. The study follows a structured review protocol with three researchers and searches major scientific databases (Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE) Xplore, ScienceDirect, Springer Link, and Wiley) over a 2002–2019 publication window using CR/TB/exercise-related keywords. Based on the extracted evidence, the authors develop a taxonomy for CR systems and evaluate the literature with emphasis on architecture and scenarios, while also considering capabilities, roles, tools, and evaluation criteria. A substantial contribution is the dedicated "Tools" chapter, which organises and compares the concrete tools and mechanisms reported across the reviewed platforms, including emulation, simulation, hardware, management, monitoring, traffic generation, user-behaviour generation, scoring, scenario definition, and security testing, with detailed tables for each category. The paper highlights commonly reported choices such as monitoring tools (e.g., Tcpdump, IP Flow Information Export (IPFIX), Wireshark), emulation tools (e.g., VMware and Emulab), and simulation tools (e.g., Qualnet, Simulink, Network Simulator, Matlab), and it also discusses the role of physical components (e.g., Cisco-based devices and programmable logic controller (PLC) devices) in several TBs. Finally, the authors synthesize the reviewed architectures into a unified functional architecture (e.g., portal, management, training/education, and testing modules) and discuss observed trends such as a shift toward dynamic scenarios and increasing automation.

We build on this literature review by examining publications from 2020 onwards and by placing a similar primary emphasis on the technologies used in CRs and TBs.

2.1 Definitions

In the surveyed literature, several slightly different definitions of CRs and TBs are used. Based on our collected data, some of these definitions no longer appear accurate. For example, Ukwandu et al. [189] differentiate CRs and TBs by arguing that CRs are mostly applied in IT environments, whereas TBs are preferred in OT environments. Our current analysis suggests that this distinction no longer holds, as discussed in Section 4.2. In addition, Kampourakis et al. [71] describe TBs as infrastructures that typically serve a predefined functional purpose, in contrast to CRs. In the same line of argument, they describe a CR—similar to Yamin et al. [208]—as an environment that provides such TBs. Chouliaras et al. [38] note that multiple definitions of CRs exist in the literature. As a pragmatic reference point, they adopt the definition from the National Institute of Standards and Technology (NIST) one-pager [118] as a "first among equals." This definition emphasizes interactive and simulated representations of an organization's networked environment that support hands-on skill development as well as product development and security testing. However, our research indicates that CRs are not limited to purely simulated infrastructures. Instead, they may also integrate physical components, for example via hardware-in-the-loop (HiL) systems that connect real devices with simulated environments. Based on these observations, we propose updated definitions of CRs and TBs that reflect a technology-centreed perspective and are grounded in the empirical evidence collected in this study.

Definition (Cyber Range). A CR is a technology stack for constructing one or more isolated virtual or hybrid digital infrastructures for purposes such as training, education, research, testing, and experimentation.

Definition (Testbed). A TB is an isolated digital infrastructure environment that can be virtual, physical, or hybrid, designed for training, education, research, testing, and experimentation.

Relationship between cyber ranges, testbeds, and digital twins. In our terminology, a CR instantiates one or more *target infrastructures*, which can take the form of TBs and/or digital twins.

3 Methodology

This chapter describes the approach used for data collection and literature review. First, we outline the search strategy used to compile the initial literature list. This is followed by a description of the criteria applied to filter this initial list to form the knowledge base for this work. Finally, we detail which data points were extracted from the collected articles.

3.1 Search strategy

To gain a comprehensive overview of technologies used in CRs and TBs, the search criteria for the literature review were deliberately broad. This is reflected in the search string. Although the focus is on technologies used, all articles on security, CRs, and TBs from all application domains were considered. To cover this broad scope, a search string was composed containing the terms "Cyber Range(s)", "Testbed(s)", "Cybersecurity", "cyber defense", and "IT Security". The final string was formulated as:

```
cyber range(s) OR testbed(s)
OR test bed(s) AND cybersecurity OR
cyber security OR cyber defense
OR it security
```

For the literature search, the following search engines were used: Science Direct, ACM Digital Library, and IEEE Xplore. This work builds upon the article by [208], which examined publications up to the end of 2019. Therefore, the first filter applied was the examination period from 2020 to August 2025. The remaining publications were then primarily pre-filtered based on inclusion criteria and abstracts. This process yielded 631 publications identified in our systematic literature review, which were then filtered according to inclusion and exclusion criteria. A total of 199 articles were ultimately included in the study.

Inclusion criteria:

- The publication must relate to security and computer science domains. This includes, but is not limited to, Internet of Things (IoT), supervisory control and data acquisition (SCADA), and cyber-physical systems (CPS).
- The publication must significantly focus on CRs and/or TBs or dedicate a considerable portion of its content to these topics. It should provide adequate technical documentation of the technological components, system design, and implementation details rather than offering purely conceptual discussions.
- The publication must be written in English.

Exclusion criteria:

- Secondary and tertiary literature, such as surveys, reviews, and similar publications, were excluded.
- TBs from domains other than computer science were excluded.
- TBs focusing on security of structures and security/safety of persons were excluded.
- TBs that primarily consist of hardware were excluded.
- Conference abstracts, book reviews, conference information, extended abstracts, discussions, proposals, editorials, mini reviews, news, and short communications were excluded.
- Publications not available in electronic form were excluded.
- Books, technical reports, lecture notes, presentations, reviews, and theses were excluded. In these cases, the corresponding conference or journal publications were reviewed if available.
- Studies that do not specify concrete technologies or provide insufficient description of the technologies discussed will be excluded from the review.

3.2 Data selection and quality assessment

This chapter explains the methodology and structuring of the information collection process in more detail. It also describes the quality criteria applied to both the selection of publications and the extraction of technology data. To answer the research questions, we collected information from the publications themselves and from the infrastructure described in them, namely CRs and TBs as well as the related technologies. Figure 1 provides an overview of the collected information objects and how they are structured. Due to the large volume of content, examples of specific instances of these categories are not described here but are presented in Section 4, and a condensed version of the data repository is also provided in Appendix A. The fields highlighted in blue indicate the areas where information was actively collected, while the non-highlighted fields contain additional information that was not categorized. The fields shown in gray represent the category names that were developed to classify and structure the technologies and infrastructures. These categories are explained in this chapter and are used consistently throughout this work. For the development and naming of the categories, we first extracted the relevant information from each publication and recorded it in a consolidated list while preserving the original wording used in the source. Next, we semantically grouped the extracted items to derive category definitions and labels. We then used these categories to harmonize terminology across publications and to map each item to the final set of categories used in the analysis.

Study-level quality criterion

Beyond the formal inclusion and exclusion criteria described in Section 3.1, the full-text review applied an additional quality threshold at the study level. Papers were assessed for

whether they provided sufficient and unambiguous technical detail to support meaningful data extraction. Publications in which technologies were mentioned only in passing, without description of their role in the CR or TB, were excluded even if they formally satisfied the inclusion criteria. This criterion addresses the practical quality dimension of data extractability, i.e., whether a paper yields structured and attributable evidence for answering the research questions.

In virtualized infrastructures, a wide variety of technologies are used. To maintain clarity and analytical focus, we limited the entries in our list to technologies that are directly relevant to building the CR or TB and to realizing the respective *use cases*. The following paragraphs therefore explain the scope decisions and constraints applied when compiling the final technology list.

Implementation requirement

Technologies that were only mentioned in related work or discussed as potential options but not actually implemented were excluded from this analysis.

Relevance to CR/TB purpose

Similarly, we did not include ubiquitous, general-purpose software or protocols that are not specifically designed for CRs or their *use cases*. This exclusion applies to common operating systems like Windows or Linux, standard data formats such as .txt or .exe, and widely used protocols like Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Hardware inclusion criterion

Physical devices and hardware were also excluded unless they are essential for scenario realization and explicitly described in the corresponding publication (e.g., a realtime digital simulator (RTDS) in the industrial control systems (ICS) domain).

Reusability criterion

Custom scripts and ad hoc programs were not added. However, we did include the development frameworks and libraries used to create them, as these components are reusable and comparable across studies.

3.2.1 Infrastructure

Application Areas

The *Application Areas* represent the environment for which the CR or TB was developed. Examples include ICT and ICS. We first adopted the labels exactly as described in each publication. We then harmonized semantically similar labels and retained as top-level categories those that occurred most frequently to ensure consistency across sources. Although CRs and TBs can support multiple *application areas*, the publications typically focus on a single one. Therefore, in this work, each publication and its described infrastructure were assigned to only one *application area*. For a more fine-grained classification, we subdivided these *application areas* into *Focus Areas* using the same procedure.

Purposes

Yamin et al.'s study on CRs and security TBs [208] identifies *Testing*, *Education*, and *Experiment* as CR purposes. The authors report that, over time (up to 2019), testing scenarios received increasing attention. In a 2021 survey of technical directors or managers directly involved with a CR, Chouliaras et al. [38] asked about the purposes of CRs and TBs and reported the following responses: *Research*, *Training*, *Exercise*, *Education*, *Testing*, and *Education Labs*. Most respondents indicated *Training* as the primary purpose. Katsantonis et al.'s CR design framework paper [76] distinguishes three types of CRs based on aims and objectives. *Educational* CRs are used for education and training and provide an organised learning environment for hands-on cybersecurity practice. *Certification* CRs assess and certify participants' cybersecurity knowledge and skills, often through competitions. *Test* CRs are used for research and for testing cybersecurity products (technologies, tools, etc.). Kampourakis et al.'s reference architecture study [71] similarly argues that *education* and *competence building* are key focuses of CR purposes. The authors group purposes into *Education*, *Research*, and *Competence Building*. They further subdivide *Research* into *Testing* and *Experimentation*, and *Competence Building* into *Training*, *Assessment*, and *Classification*. Based on the publications we analysed, we consolidated the identified *use cases* into three *purpose* categories: *Research, Testing and Experimentation*, *Training and Exercises*, and *Education*. This set of *purposes* is aligned with the surveys described above. Individual *use cases* further refine each *purpose* into more specific categories and were extracted from the context of each publication and then clustered. Several of the reviewed publications focus on the construction and design of CRs or TBs for specific objectives. Because technology selection often involves goals such as cost-effective CR design or scalability and performance optimization, we introduced the *System Architecture and Implementation* category as an additional filter for the technology selection guideline.

Architectural Layer

The literature reports several variants of the structural organization of a CR. Kampourakis et al. [71] describe distinct *zones* in which the modules mentioned in Section 3.2.1 are situated. The *Target Infrastructure Zone* lies within the *Core Infrastructure Zone* and denotes the infrastructure instantiated by the CR. This may be a TB or a digital twin. The *Underlying Infrastructure* constitutes the backbone of the CR, comprising hardware, software, servers, and networking, and represents the infrastructure on which the CR is deployed. Also within the *Core Infrastructure Zone* are the *virtualization* and *orchestration* zones. Here, tools such as OpenStack, Docker, or VMware are used to instantiate virtual

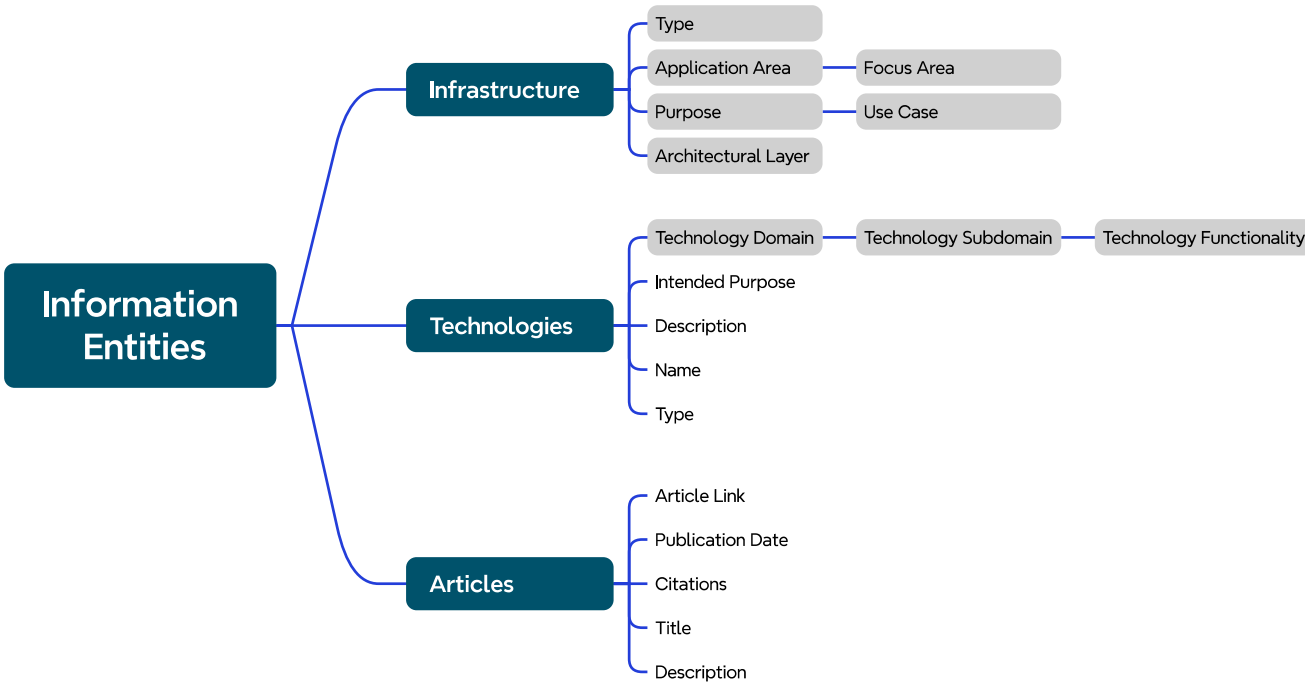


Fig. 1 Organised overview of information and categories derived from publications

machines and to orchestrate systems with tools like Ansible or Terraform. Technologies of this kind form the computing platform of CRs. Outside the Core Infrastructure Zone, the *learning management and support zone* provides services and tools for instructors and learners, as well as technologies for creating, customizing, and deploying scenarios, tactics, techniques, and procedures (TTPs), and for traffic generation. The *monitoring and management zone* contains user and scenario monitoring modules, while the *access control zone* comprises authentication and authorization modules. According to Ukwandu et al. [189], emulation, simulation, virtualisation, and containerisation constitute the core technologies of a CR. Above these sits the *orchestration layer*, which includes infrastructure technologies such as vSphere and Wisper. The *CR capabilities layer* encompasses functionalities and capabilities as outlined in Section 3.2.1, and the *front-end technologies layer* provides the user interface of the CR. To position technologies within architectural zones or layers, we grouped the functionalities into four layers (see Figure 2). The figure not only illustrates the layer structure but also highlights the most frequently mentioned *technology domains* within each layer.

The *Underlying Infrastructure* layer comprises the hardware on which the CR or TB is deployed. This may include servers, cloud-provider hardware, distributed hosts, a single host, or other suitable devices. This layer is included for completeness but is outside the scope of this work. The *Core Technology Layer* primarily includes computing-platform technologies used to instantiate the target infrastructures of the CR. Typical examples are cloud infrastructure tools such as OpenStack, AWS, or Google Cloud, virtualization platforms with Type 1 and Type 2 hypervisors such as VMware vSphere or VirtualBox, and containerization technologies such as Docker. The *Orchestration Layer* covers container-orchestration tools such as Kubernetes, software and infrastructure provisioning and configuration tools such as Ansible and Terraform, and data formats such as YAML (YAML Ain't Markup Language). These can be used as scenario specification and description languages and support automated instantiation of the target infrastructure. The top layer consists of one or more *Target Infrastructures* and contains all technologies and functionalities required to realise the respective *use cases*.

It is important to note that technologies and functionalities cannot always be clearly assigned to just one layer in every CR. For instance, Nelson et al.'s CR [120] uses QEMU, which is a virtualization technology, inside a Docker container. In this scenario, Docker is considered part of the Core Technology Layer, while QEMU is assigned to the Target Infrastructure Layer. Another example is data storage technologies such as relational databases. These can be found in the Target Infrastructure Layer, where they serve as training systems for structured query language (SQL) injection exercises in red-teaming scenarios, as described by Vasilakis et al. [192]. Additionally, the literature presents integrated CR solutions and related tools that cover multiple layers. As a result, they can be placed in more than one part of the architecture.

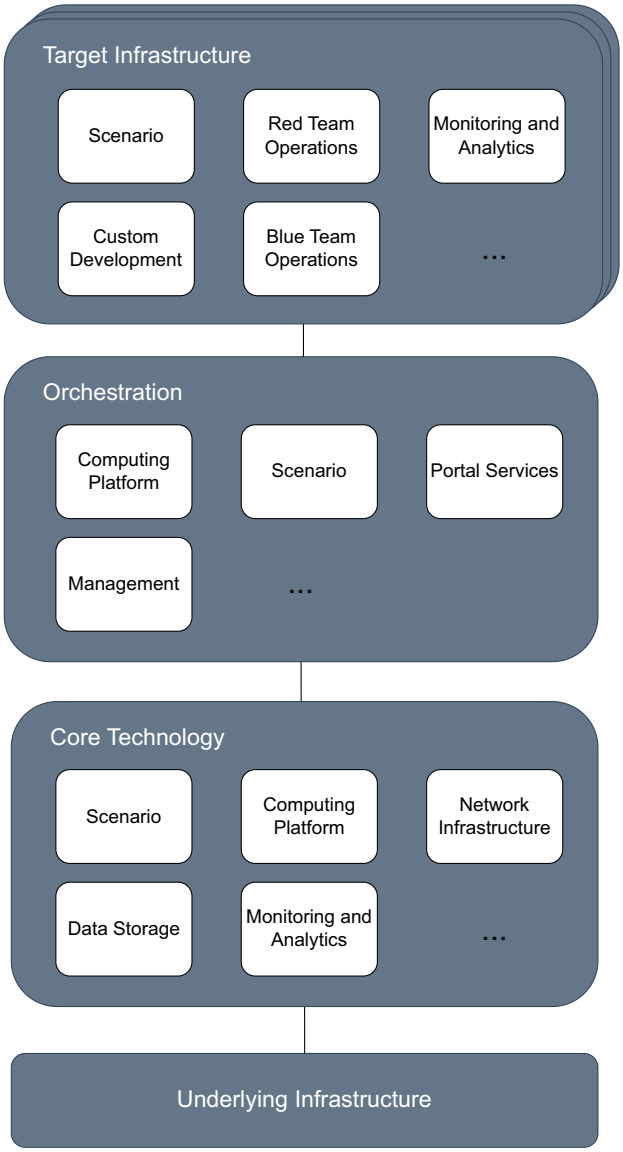


Fig. 2 Layered architecture of a cyber range with exemplary features per layer

Technologies

From the reviewed publications, we also identified and categorized the technologies used in CRs and TBs. The selected technologies determine the functionalities and capabilities of the CR or TB. Kampourakis et al. [71] group CR functionalities into modules, including *Scoring & Reporting*, *Users & Scenario Monitoring*, *Data Collection & Analysis*, *Assets Monitoring*, *Scenario Development*, *Traffic Generation*, and many others. Yamin et al. [208] similarly decompose the functional architecture into modules and submodules. Examples include *Management* (for CR, scenario, exercise, or test) and *Portal* (for user, admin, or client). Ukwandu et al. [189] and the European Cyber Security Organisation (ECSO) report *Understanding Cyber Ranges: From Hype to Reality* [57] provide illustrative lists of functionalities and capabilities that a CR may offer. These include instructor tools, Internet services simulation, attack simulation, competency management, visualization, reporting, and training methods. Both sources emphasize that the examples are not exhaustive and that a CR does not need to implement all listed functions. Aligned with the terminology used in these publications and based on the identified technologies, we constructed a hierarchical taxonomy comprising a *Technology Domain* category with 10 entries and a *Technology Subdomain* category with 81 entries, as well as a *Technology Functionality* category that specifies the precise *purpose* of each technology. In addition, we categorized the *technology type* as one of the following: tool, data format, framework, library, OS, platform, protocol, or technology stack. *Articles*

For each publication, in addition to the title, year, and link, we added all relevant fields to the list. From the official websites of each technology, we extracted the website link, the original intended use, and a short description, because the intended use within CRs can differ from the technology's primary *purpose*. For the CRs and TBs themselves, we also extracted a concise description from the publications.

4 Results

In this chapter, we first present the findings of the literature survey and then, based on the categories and structures established for CRs and TBs, explain how different functionalities are realised within the respective domains and *use cases*. The chapter concludes by highlighting dependencies and requirements across *use cases*, as well as gaps in specific research topics.

4.1 Literature survey

The stacked bar chart (Figure 3) summarizes the distribution of 199 unique publications on CRs and TBs, across CR & TB *application areas* for 2020–2025. Overall publication activity increases from 14 papers (2020) to 28 (2023), followed by a pronounced peak in 2024 (60) and a still-high volume in 2025 (49). Across the full period, ICT dominates with 64 papers (32.2%), followed by ICS (37; 18.0%), Power Systems (27; 13.0%), and CPS (25; 12.0%). Smaller but visible areas are IoT, Industrial Internet of Things (IIoT) (19; 9.5%), radio access network (RAN) & Mobile Devices (14; 7.0%), and Intelligent Transportation Systems (13; 6.5%).

4.2 Cyber range and testbed purposes and use cases

Figure 4 visualizes the distribution of identified publications across *application areas*, *purposes*, and infrastructure types of CRs and TBs using a Sankey diagram. On the left, the

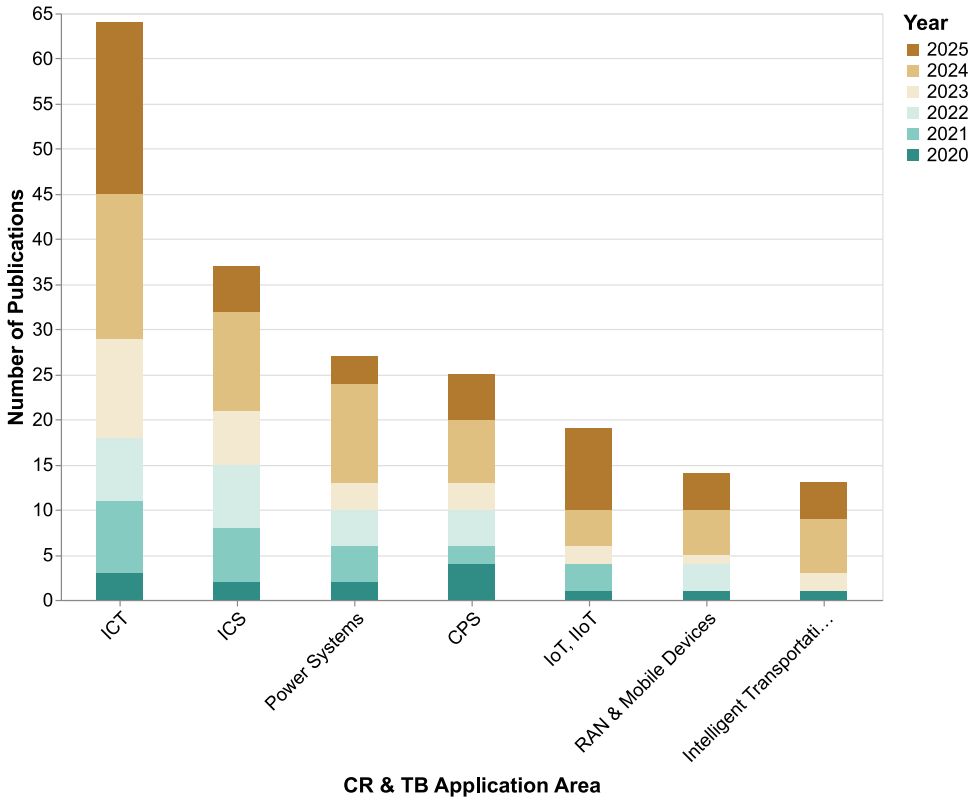


Fig. 3 Publications per Application Area

CR & TB Application Areas (for example, ICT, ICS, CPS, IoT/IIoT, Power Systems, Intelligent Transportation Systems, and RAN & Mobile Devices) are listed. In the middle, the three overarching *purpose* categories, namely Education, Research, Testing and Experimentation, and Training and Exercises, are shown. On the right, the Infrastructure types (CR and TB) are displayed. The width of the links between nodes is proportional to the number of distinct publications that describe at least one *use case* for the respective combination of *application area*, *purpose*, and infrastructure type. Each publication is assigned to exactly one *application area* and exactly one Infrastructure type (either CR or TB), but it may address multiple *purposes*. Consequently, a publication in the ICT domain can appear in several *purpose* categories, yet it is never assigned to multiple infrastructure types in parallel. In the analysis, a publication may therefore be counted multiple times across *purpose* categories, but at most once per combination of *application area*, *purpose*, and infrastructure type. The analysis reveals that the *purpose* Research, Testing and Experimentation (RTE) is most prominent in the ICT *application area*, with a total of 41 publications (18 using CRs and 23 using TBs). In contrast, the *purposes* Education and Training and Exercises in ICT are predominantly implemented using CRs, with 14 of 15 Education publications and 21 of 22 training-related publications relying on CR-based environments. In ICS, RTE spans 29 publications (3 CR and 26 TB), while Training and Exercises is represented in 13 publications distributed almost evenly between CR (7) and TB (6). Other domains, including CPS, IoT/IIoT, Power Systems, and Intelligent Transportation Systems, display a strong dominance of TBs in RTE contexts. In some cases (for example, Intelligent Transportation Systems), CRs do not appear at all. Overall, the Sankey diagram highlights that RTE is the predominant *purpose* across most *application areas* but is mainly realised using TBs. CRs are used particularly in ICT (and partly in ICS and RAN & Mobile Devices) for Training and Exercises and educational *purposes*.

4.2.1 Research, testing and experimentation

Figure 5 summarizes the top-10 *use cases* reported for the "Research, Testing and Experimentation" *purpose* across CRs (CR) and TBs (TB). Because a single article may describe multiple *use cases*, the bars count use-case mentions rather than unique papers. The dataset contains 305 total mentions. The ten most frequently cited *use cases* account for 171 mentions (56.1%). All remaining *use cases* are each mentioned fewer than five times and are therefore not shown in the figure. Together they account for 134 mentions (43.9%). Across platform types, TB dominates with 257 mentions (84.3%), followed by CR with 48 mentions (15.7%). Among the individually named *use cases*, "Threat and Vulnerability Assessment" leads with 46 mentions, followed by "Attack Impact Assessment" (35)

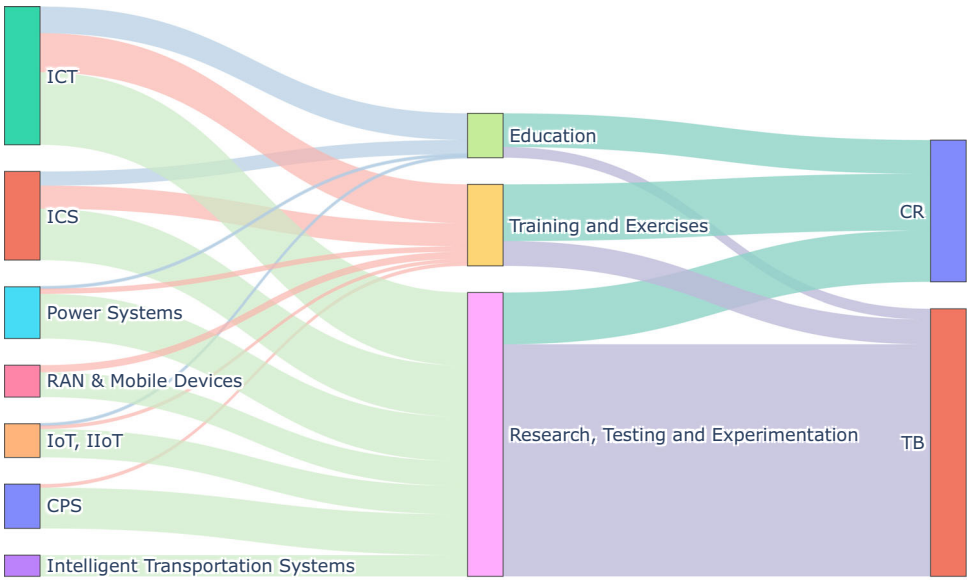


Fig. 4 Distribution of cyber range and testbed *application areas* across purposes and infrastructure types

and "Dataset Generation" (29). The next tier comprises "Cyber Security Resilience Assessment" (18) and "Mitigation Strategies" (10). Additional, lower-frequency *use cases* include "machine learning (ML)-based intrusion detection system (IDS)/intrusion prevention system (IPS)" (9), "Anomaly Detection" (8), and "artificial intelligence (AI)-based Anomaly Detection" (6), with both "Cyber Security Risk Assessment" and "Traffic Generation" completing the top-10 at 5 mentions each. Overall, evaluation-oriented activities (threat/vulnerability and impact assessments) dominate, complemented by dataset generation and resilience testing, while detection- and ML-focused *use cases* appear consistently but with smaller absolute counts.

Threat and Vulnerability Assessment

An experimental security-testing setup for IoT and web applications deploys a target environment that is systematically scanned and probed using tools such as Acunetix, generating traffic and findings that are used to assess vulnerabilities and misconfigurations present in the TB [115]. A security TB for next-generation systems integrates external threat-intelligence feeds such as URLhaus with a controlled environment, using the collected malicious Uniform Resource Locators (URLs) to retrieve and analyse malware-related content and thereby evaluate how well different defensive mechanisms perform in detecting and handling these threats [112].

Attack Impact Assessment

A cyber-physical security simulation TB for distribution networks combines power-system models in RTDS with Network Simulator 3 (ns-3)–based communication and Modbus-linked SCADA control, enabling cyberattacks on the control layer whose consequences on voltages, currents, and other power-system variables are examined to assess the impact of different attack scenarios [170]. In a digital power-twin environment for smart grids, attacks are launched against grid components represented both in the physical TB and in the real-time digital twin, and their impact is assessed by analysing anomaly alerts carried via International Electrotechnical Commission (IEC) 61850 Generic Object Oriented Substation Event (GOOSE) messages and the corresponding changes in grid operation within the twin [74].

Dataset Generation

The SDN-DAD dataset is generated in a software-defined networking (SDN)-based test environment by orchestrating benign Hypertext Transfer Protocol (HTTP) traffic, flash events, and multiple distributed denial-of-service (DDoS) attack types using curl-loader and other tools, capturing controller and flow-level information so that the resulting dataset can support research on efficient DDoS detection features [77]. A log-data–oriented TB for cybersecurity experiments uses scripted user interactions driven by Selenium and controlled system activities to produce realistic, reproducible log traces, which are then released as publicly available datasets intended for training and evaluating intrusion-detection and analytics approaches [188].

Cyber Security Resilience Assessment

A resilience-focused TB models a truck equipped with an autonomous cyber-defence system and physical resilience mechanisms, and uses OpenTAP to automate malware-attack experiments so that quantitative cyber resilience metrics can be derived from how the combined cyber and physical safeguards maintain functionality under sustained compromise attempts [202]. Another study on protection intelligent electronic devices (IEDs) uses a laboratory setup with IEC 61850 GOOSE communication to mount protocol-level attacks and observe device responses, thereby assessing the resilience of different commercial IED implementations in terms of their

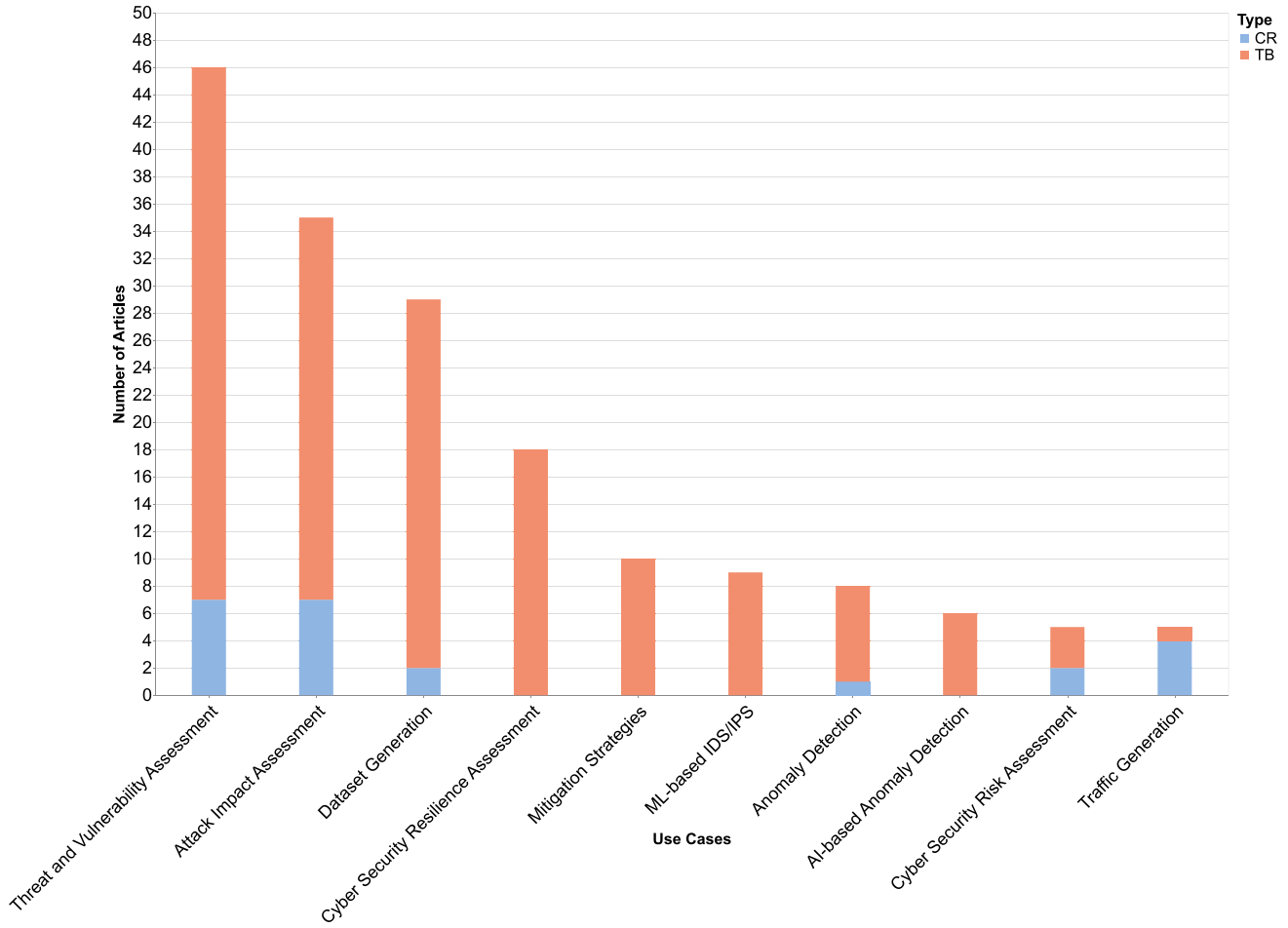


Fig. 5 Top-10 use cases reported for the "Research, Testing and Experimentation" purpose across cyber ranges (CR) and testbeds (TB)

ability to withstand, detect, and recover from GOOSE-based disturbances [25].

Mitigation Strategies

In the hierarchical SDN DDoS defence TB, the generated SDN-DAD traffic is used not only for detection but also to evaluate mitigation strategies coordinated across controllers, where the system dynamically adapts flow rules based on the detection outputs to limit attack traffic while preserving legitimate flash-crowd requests [77]. A real-time co-simulation TB for public electric vehicle (EV) charging links an OPAL-RT HYPERSIM-based power-grid model with EV infrastructure and a monitoring platform, allowing the authors to inject EV-based cyberattacks and then assess mitigation strategies that react to abnormal grid and communication conditions in order to maintain stable operation [77].

ML-based IDS/IPS

An SDN TB targeting IoT-driven DDoS attacks embeds a semi-supervised deep learning model in the SDN controller, where traffic generated by curl-loader and attack tools is monitored and classified by the ML-based intrusion-detection component to distinguish benign from malicious flows and support automated defence decisions [141]. A power-system security environment that models oscillatory load attacks from compromised EV charging stations uses a MATLAB/Simulink implementation of the IEEE New England 39-bus system to generate cyber–physical datasets, which are then processed by deep-learning models at the edge to detect and localise the attacks as part of an ML-based IDS for the grid [155].

Anomaly Detection

A smart-grid TB built around PLCs, rapid-SCADA, pySCADA, and an SQL-backed log server supports an explainable, self-aware intrusion-detection and active-response framework, where anomaly detection is performed by analysing the collected process and communication traces from the power grid to identify suspicious behaviour and trigger automated responses [214]. In a CR platform that logs user and system activity across various services, process-mining tools are applied to event logs to discover normal process models and detect deviations, so that anomaly detection is framed

as conformance checking between observed CR execution traces and expected process behaviour [24].

AI-based Anomaly Detection

An open fifth-generation mobile network (5G)/Open Radio Access Network (O-RAN) TB is built around components such as Open5GS for the core network, an RAN Intelligent Controller (RIC), and GNU Radio / GNU Radio Companion, including a flow graph that simulates different condition levels for multiple user equipment (UEs). Within this environment, the authors introduce a novel AI-based anomaly detection approach that is evaluated on the generated traffic and is designed to maintain a near-zero false positive rate on clean traffic [129] A co-simulation TB for distributed energy resources combines real-time power-system simulation in RTDS with network emulation in ns-3 and SCADA communication over Modbus, and applies model-based reinforcement learning to detect coordinated cyber–physical attack events, treating the learned model as an AI-based anomaly detector that signals deviations from normal grid operation [153].

Cyber Security Risk Assessment

A cooperative smart-farming environment combines physical systems with digital twins at the edge, where a digital twin is implemented using Azure Digital Twins and then subjected to attacks so that cyber and digital-twin behaviour can be observed. The resulting smart-farming network datasets are used for dataset generation and AI-based anomaly detection to identify potential threats in this setting [132]. A cyber-physical security simulation TB for distributed energy resources uses Modbus communication between SCADA systems in control centres and remote terminal units together with real-time simulation of power and communication systems in RTDS and network emulation in ns-3, so that cyber security risk assessment can be performed by carrying out cyberattacks on the simulated distribution network and analysing their impact on the power system [170].

Traffic Generation

An SDN-based TB for defending against DDoS attacks launched by compromised IoT devices uses curl-loader together with other traffic tools to generate large volumes of HTTP requests and diverse DDoS patterns, so that the controller's semi-supervised detection and mitigation logic can be evaluated under mixed legitimate and attack traffic conditions [141]. A hierarchical DDoS defence system for SDN networks similarly relies on curl-loader to emulate flash-crowd HTTP traffic at scale, combining this generated workload with various DDoS attacks to build the SDN-DAD dataset and to assess how the proposed multi-layer defence behaves under different traffic and attack configurations [77].

4.2.2 Training and exercises

Figure 6 summarizes the top-10 *use cases* reported for the *purpose* "Training and Exercises" across CRs and TBs. Because a single article may describe multiple *use cases*, the bars count use-case mentions rather than unique papers. The dataset contains 75 total mentions. The ten most frequently cited *use cases* account for 47 mentions (62.7%). All remaining *use cases* are each mentioned fewer than five times and are therefore not shown in the figure. Together they account for 28 mentions (37.3%). Compared with "Research, Testing and Experimentation", where TB dominates (TB 84.3%, CR 15.7%), the "Training and Exercises" *purpose* is markedly CR-centric. CR accounts for 56 mentions (74.7%), with TB contributing 19 mentions (25.3%). Within the top-10, "Cyber Security Training: Capture the Flag" leads with 9 mentions, followed by "Cyber Security Training: General" with 8 mentions. The next tier comprises "Incident response" (6), "Cyber Security Training: Red Team vs. Blue Team" (6), and "Gamification" (6). Lower-frequency *use cases* include "Cybersecurity Exercise Evaluation" (5), "Cyber Security Training: Red Teaming" (3), and "Cyber Security Training: Malware Attack and Defense" (2), with "Crisis Management Training" and "Cellular Botnets" completing the top-10 at 1 mention each. Overall, the distribution shows that training-oriented work is predominantly conducted on CRs, with TBs providing a smaller but visible share.

Cyber Security Training: Capture the Flag

A capture-the-flag *use case* is implemented on the TROY TB, a virtual IT and OT environment hosted on a VMWare ESXi hypervisor with dedicated virtual networks and machines following an IT/OT reference architecture, where a Typhoon-HIL 602+ real-time simulator runs high-fidelity critical-infrastructure power-grid models (IEEE 4-, 13- and 33-bus using ModbusTCP or DNP3), classroom exercises use part of the GRFICSv2 framework with a graphical Tennessee Eastman process simulation, SCADA and a virtual PLC via OpenPLC, and Ignition SCADA together with OPC UA tags provides the SCADA/user interface (UI) layer, while NET-LAB+ offers snapshotting and reset of the virtual lab so that capture-the-flag tasks can be executed repeatedly in a realistic learning-lab setting [173]. A second capture-the-flag *use case* is realised in the KYPO4INDUSTRY environment, which combines Linux-based virtual machines, physical industrial devices with sensors and actuators, and multiple industrial protocols such as Message Queuing Telemetry Transport (MQTT) and REST, so that students can work through hands-on ICS exercises on realistic industrial control exercises on realistic industrial control infrastructure [31].

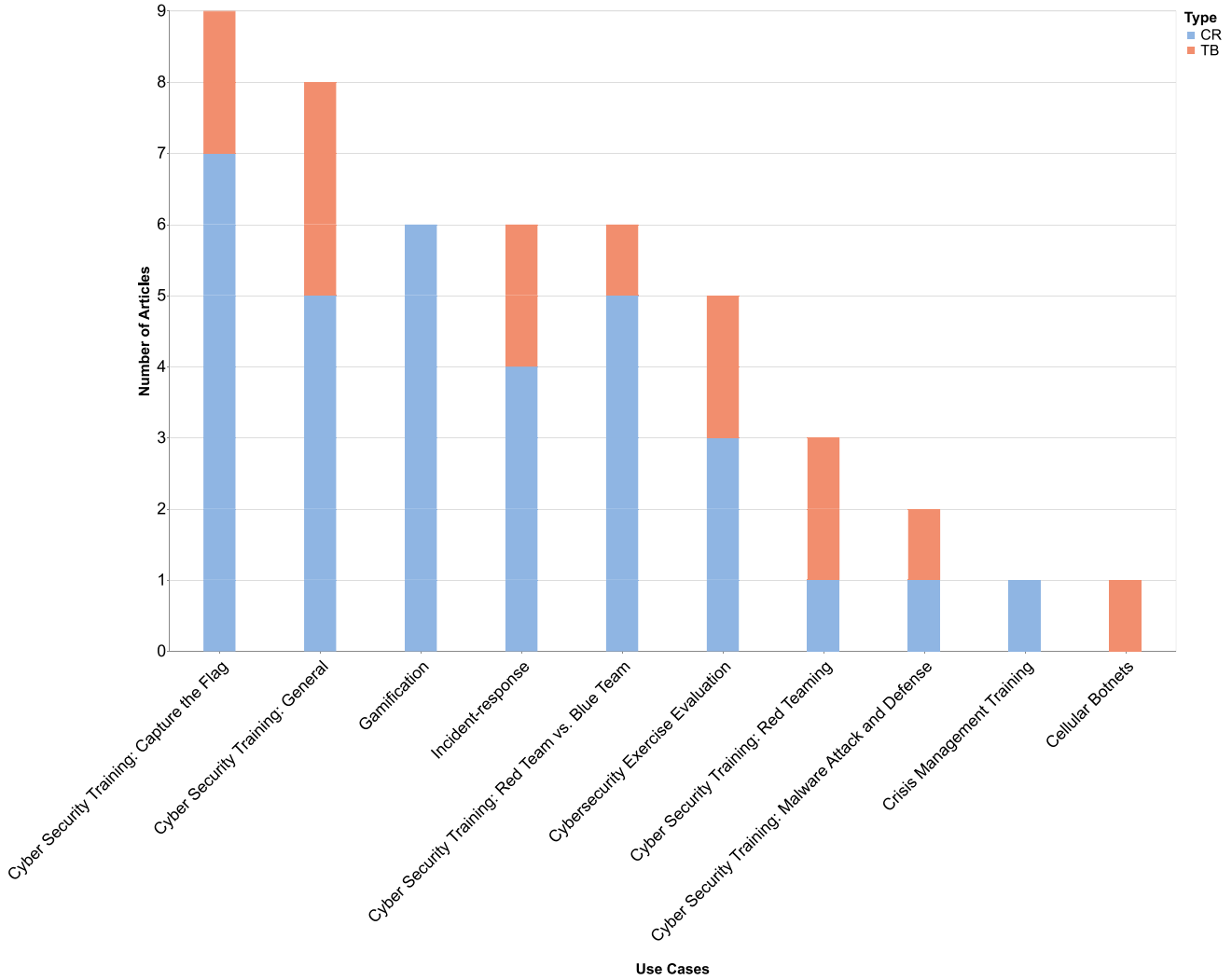


Fig. 6 Top-10 use cases reported for the "Training and Exercise" purpose across cyber ranges (CR) and testbeds (TB)

Cyber Security Training: General

A general training *use case* is based on the Austrian Institute of Technology (AIT) CR, designed as a modular OpenStack-based environment where CRs are instantiated and managed via Terraform, Consul and Git, enabling flexible deployment of different training topologies and exercises for cyber security education and practice [91]. Another general-purpose training *use case* is provided by the Tectonic academic CR, which relies on cloud infrastructure and infrastructure-as-code to deploy realistic systems and networks, integrates Elastic Security for monitoring and alerting, and supports configurable training exercises that combine theoretical teaching with practical CR activities [64].

Incident response

One incident-response *use case* is realised in a wastewater-treatment IoT TB, where IoT devices publish their state via MQTT and the collected data is stored and labelled according to network activities, allowing incident handling and detection workflows to be exercised on realistic process and communication traces from the treatment environment [32]. An incident-response *use case* is realised in a CPS TB-based QRGridEx environment, where a real-time digital power-system simulator is combined with standard SCADA communications and integrated intrusion and anomaly detection systems so that cyberattacks on the grid can be launched and their detection and handling analysed across the coupled cyber–physical infrastructure [144].

Cyber Security Training: Red Team vs. Blue Team

One red-team-vs-blue-team *use case* is built around the CRACK framework, which runs on an OpenStack-based TB orchestrated via Apache ARIA and provides network-security exercises where a red team attacks multi-tier services (for example an Apache-based web server front end and internal servers) and the blue team defends and analyses these activities within the emulated infrastructure [150]. Red-team-vs-blue-team training is supported by the DefAtt platform,

a highly automated CR that deploys virtual machines and containers as networked targets and uses central logging and analysis components to run structured games focused on network-based attacks and their defences, while also enabling scalability testing of the exercise environment [104].

Gamification

In one Gamification *use case*, an industrial cybersecurity environment uses remote-access laboratories with industrial control equipment and communication infrastructure to deliver cyber security education, where gamification is achieved by turning the industrial communication and process-control tasks into structured challenges within the training setup [87]. A further gamified *use case* appears in the NITRO 5G-IoT CR, which emulates a genuine 5G core network and interconnected IoT systems and uses generated network traffic and 5G services to build game-like exercises, allowing participants to test, analyse and refine security aspects through gamified interactions with the emulated 5G–IoT environment [58].

Cybersecurity Exercise Evaluation

One *use case* for exercise evaluation uses a cyber-range framework that automates many tasks of conducting cyber security exercises, where scenarios are modelled and executed via a JavaScript Object Notation (JSON)-based domain-specific language and Datalog specifications, and CTFd is used for scoring and instrumentation so that participant performance and exercise properties can be systematically analysed [206]. Another exercise-evaluation *use case* is described in a cyber range implementation and evaluation methodology that leverages process-mining tools to analyse event logs from training exercises, using platforms such as Moodle and other monitoring components to collect data and then evaluate cyber range trainings and education processes from different perspectives [63].

Cyber Security Training: Red Teaming

A red-team training *use case* is provided by a SCADA cybersecurity awareness and training program built around two twin CRs, WonderICS and G-ICS, where an advanced persistent threat (APT) demonstrator and a flexible lab environment allow participants to practise attacking and defending industrial control setups in hands-on exercises and student pentesting sessions [136]. Dockerized Android sets up a container-based CR environment for mobile devices, where Android Emulator–based devices and related services are deployed via Docker to build realistic, vulnerable mobile scenarios for red-team exercises. A web UI with a React.js frontend and Nginx/Node.js backend provides coordinated access to these emulated devices and vulnerable applications such as the Wi-Fi Baby Monitor app, so that threat and vulnerability assessment can be carried out as structured red-teaming training *use cases* [30].

Cyber Security Training: Malware Attack and Defense

A maritime malware-attack-and-defence *use case* is realised on the MaCySTe virtual TB, which reproduces the onboard network infrastructure and core components of shipboard cyber–physical systems by interfacing with a patched Bridge Command ship simulator that exchanges simulation data via a message-queuing setup, while a data collection unit and radar antenna transmit sensor data as multicast UDP using National Marine Electronics Association (NMEA) and BR24/Asterix protocols. The environment combines PLC simulation with OpenPLC over Modbus, FUXA-based human–machine interfaces (HMIs), radar-overlay functionality via NATS and OpenCPN, and containerised services deployed with Podman, Flatpak, GNU Make task automation and OpenSearch-based indexing, enabling realistic cyber security training for maritime operators focused on maritime cyber threats and impact assessment within a dedicated TB [99]. A CR smart-assistant environment is used for malware-attack-and-defence training, where students interact with the CR through a Yandex.Dialogs–based interface that serves as the front end for requesting educational material and receiving guidance from a virtual assistant backed by a cyber security ontology, so that training activities can be supported and assessed across learning management, instructional design and student scoring *use cases* [213].

Crisis Management Training

Crisis-management training is implemented in a CR built on OpenStack, where multiple Windows 10 client machines, servers (including File Transfer Protocol (FTP) and Virtual Network Computing (VNC)-based management access), and monitored endpoints generate realistic network traffic, and a dedicated traffic-generation setup is used so that organisations and decision-makers can be trained in crisis response and decision-making under simulated cyber incidents [149].

Cellular Botnets

A cellular-botnets *use case* is implemented on the VET5G virtual end-to-end 5G network TB, where containerized 5G core network functions, gNodeBs (gNBs) and UEs are orchestrated with Kubernetes and Docker, UEs are emulated using Android Emulator instances running Android 11 with 5G support, and components such as OAI's gNB emulator, a P4 BMv2 software switch, Open Authorization (OAuth) 2.0–based service access, MongoDB, Wireshark, tcpdump, Bettercap, Metasploit, Hydra, sFuzz, wfuzz and JupyterHub are combined to support cyber security exercises labelled "Slicing Attacks, Cellular Botnets" for attack impact assessment and testbed design and evaluation within 5G and sixthgeneration mobile network (6G) security *use cases* [204].

4.2.3 Education

Figure 7 summarizes the Education *use cases* observed across CRs (CR) and TBs (TB). Because a single article may

describe multiple *use cases*, the bars count use-case mentions rather than unique papers. The dataset contains 43 total mentions spanning five *use cases*. Across platform types, CRs dominate with 34 mentions (79.1%), followed by TBs with 9 (20.9%), indicating that education-oriented activities are most often conducted on CRs. Among the individually named *use cases*, "Student Assessment & Scoring" leads with 15 mentions and is observed exclusively on CRs. "Learning Management System" follows with 13 mentions, and "Instructional Design" records 12, with both appearing primarily on CRs but also represented on TBs. Lower-frequency activity includes "Learning Labs" with 2 mentions (observed on TBs) and "Resource Development" with 1 mention. Overall, Education *use cases* are primarily implemented on CRs, with TBs contributing mainly to learning-management and instructional-design work and covering the limited learning-labs activity.

Student Assessment & Scoring

A CR smart-assistant service is developed based on the analysis of students' digital footprints, and it provides educational material and advice through an interactive request–reply interface [213]. The BUTCA CR implements an event-based data collection and analysis *use case* on an OpenStack-operated platform, including an authentication server and proprietary web applications for platform management and cybersecurity use cases. Monitoring and dashboards are supported with Prometheus and Grafana. Orchestration is provided via Ansible AWX, and centralized log management uses Kibana with Elasticsearch. After analysis, the evaluated data are delivered to the web user interface in JSON for instance and use-case overview with client-side rendering [89].

Learning Management System

The CR system automates many tasks of cyber security exercises and supports the autonomy and skill improvement of participants. It relies on an open-source OpenStack-based deployment approach that can run on cloud infrastructures without relying on third-party infrastructure [206]. IoT security training is organised through a methodology that targets an in-depth understanding of IoT via hands-on practice. FIT IoT-LAB is used as the TB infrastructure for IoTrain-Lab in this learning-management context [18].

Instructional Design

An Industry 4.0 CR platform is developed to support exercises such as Snort ruling, forensic analysis, and man-in-the-middle spoofing. The environment uses an isolated network infrastructure with virtual private network (VPN) access to trigger alerts and generate log files for these activities [192]. An interdisciplinary approach is applied to design CR exercises and to introduce a cyber range exercise (CRX) for incident response. The learning management system is implemented with VueJS and connected to the Docker infrastructure via a REST application programming interface (API) implemented with Flask [60].

Learning Labs

TROY is proposed as a multi-faceted cybersecurity TB to address data and workforce scarcity, and it is used to compare open-source cybersecurity datasets and TBs. The learning-lab context is discussed alongside lab environments using a hypervisor managed with vSphere and NETLAB+ networking lab tools [158]. The TROY TB provides a virtual IT and OT environment equipped with a Typhoon-HIL real-time simulator for critical infrastructure emulation. IEEE 4-Bus (ModbusTCP or DNP3) and IEEE 13-Bus configurations are used as power-topology standards in this lab environment [173].

Resource Development

An OT-focused CR is developed using VirtualBox-based virtual machines. Windows 10, Ubuntu, and Kali Linux run as virtual machines on VirtualBox in this resource-development setup [154].

4.3 Technologies

This section outlines technologies and their *use cases* in CRs and TBs. Given the extensive number of technologies and publications, each subdomain presents up to two of the most widely used technologies, each described by up to two publications. At the start of each *technology domain* chapter, a heatmap visualizes the quantity and diversity of technologies discussed within that domain. At the end, a summary table lists the top technologies per subdomain. In total, 10 *technology domains* are covered, spanning the three layers of CRs or TBs: Core Technology, Orchestration, and Target Infrastructure. These domains include Red Team Operations, Data Storage, Monitoring and Analytics, Computing Platform, Custom Development, Blue Team Operations, Portal Services, Management, Network Infrastructure, and Scenario.

4.3.1 Red team operations

Overall, ICT dominates the use of Red Team Operations technologies with 116 occurrences, followed by ICS (70) and IoT/IIoT (56). Power Systems (27), RAN & Mobile Devices (24), and CPS (19) appear less frequently, while Intelligent Transportation Systems (3) is only sparsely represented. ICT reports non-zero values in all 13 Red Team Operations subdomains, and ICS, IoT/IIoT, and RAN & Mobile Devices each cover a broad set of subdomains, which indicates that these *application areas* are common targets for Red Team Operations experimentation. Across all *application areas*, Training and Practice Systems (70), Network Scanning and Reconnaissance (61), and Exploitation and Attack Execution (59) are the most frequently reported subdomains. ICT alone accounts for 28 occurrences in Training and Practice

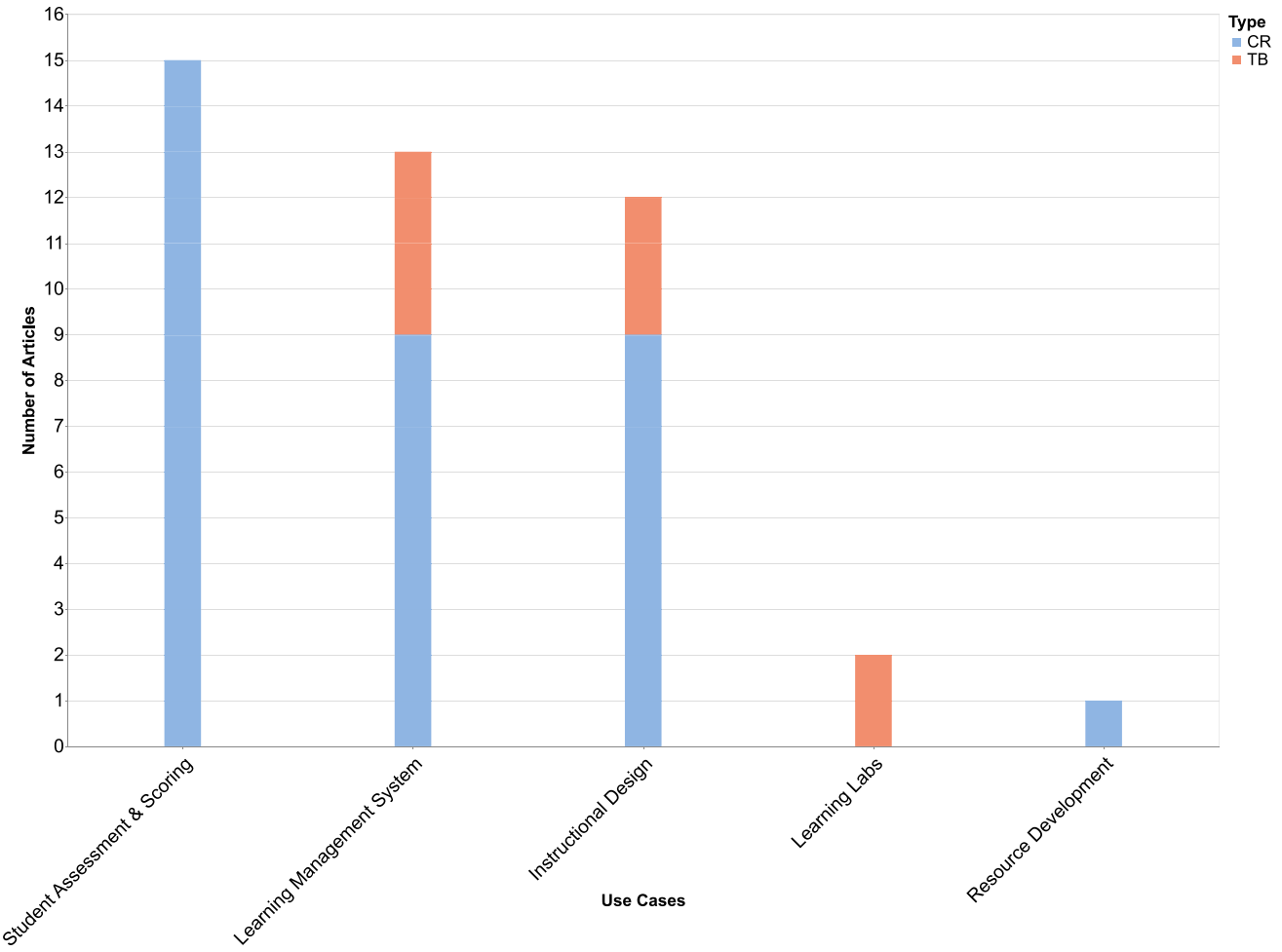


Fig. 7 Top use cases reported for the "Education" purpose across cyber ranges (CR) and testbeds (TB)

Systems, and 18 occurrences each in Network Scanning and Reconnaissance and Exploitation and Attack Execution. ICS contributes additional counts in the same subdomains with 18 in Training and Practice Systems, 14 in Network Scanning and Reconnaissance, and 15 in Exploitation and Attack Execution. In addition, Attack Strategy & Support (31), Denial of Service & Distributed Denial of Service (29), and Packet-manipulation (18) appear regularly, mainly in ICT, ICS, and IoT/IIoT. A secondary cluster is formed by Vulnerability Management (14), Password Cracking and Credential Harvesting (11), and Brute force attacks (9). More specialised activities remain rare. Adversary emulation (5) and Reverse Engineering and Binary Analysis (4) occur only sporadically, and Phishing and Social Engineering (2) as well as Proxy and Web Interception (2) are nearly absent. Taken together, the heatmap 8 shows that the analysed CRs and TBs primarily support training activities plus reconnaissance and exploitation focused Red Team Operations, while adversary emulation and social engineering activities are much less represented in the literature.

Training and Practice Systems

MySQL is used to host applications for SQL injection exercises, enabling trainees to practise detecting and exploiting injection flaws in an ICS-oriented CR [192]. The CRACK CR framework includes an Apache web server in a network security scenario where a misconfigured reverse proxy is exploited, allowing trainees to practise reconnaissance and exploitation workflows against a web front-end that provides access to internal services within the emulated infrastructure [150]. In a Raspberry-Pi-based CR, Damn Vulnerable Web Application (DVWA) is deployed as a sample vulnerable web application to assess how effectively the range supports web-application threat and vulnerability assessment exercises, letting learners perform attacks and defences in a compact training setup [138]. A distributed IoT/IIoT TB architecture integrates DVWA as a vulnerable web front end for specific scenarios in the TON_IoT datasets, where offensive systems attack the application using different techniques so that labelled telemetry and network-traffic data can be recorded for AI-based security evaluation [111].

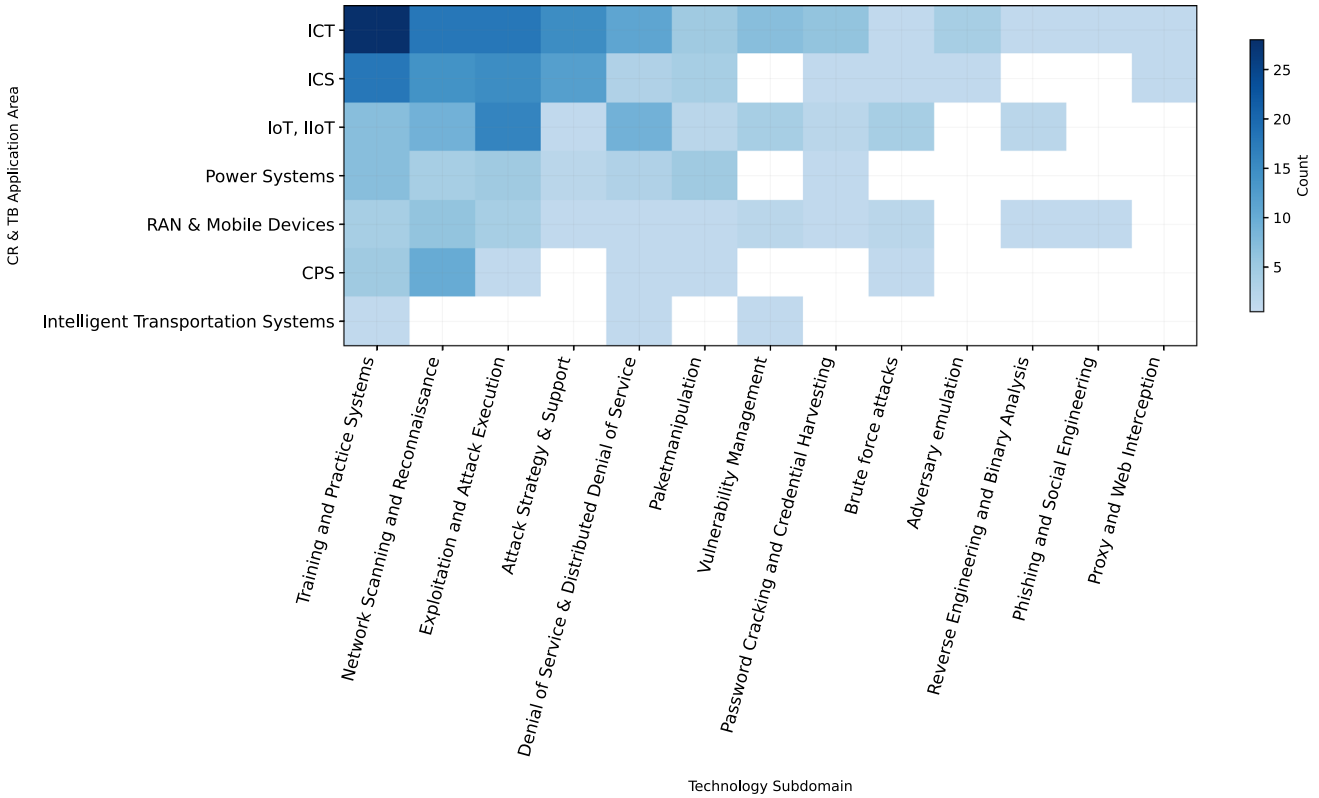


Fig. 8 Red Team Operation Subdomain Distribution Across Cyber Range Application Areas

Network Scanning & Reconnaissance

A drone-surveillance defence study uses Nmap and Wireshark for network scanning and reconnaissance: Nmap performs detailed scans of the identified target drone, while Wireshark captures and analyses the associated network traffic within the drone-surveillance TB environment to support assessment of attack effectiveness and defensive measures [197]. An emulated industrial-control TB for analysing advanced cyber threats employs Nmap to discover vulnerabilities in ICS components and Wireshark to monitor and analyse demilitarised zone (DMZ) network traffic, enabling the identification of suspicious communication patterns in realistic ICS scenarios [52].

Exploitation and Attack Execution

An anomaly-detection study for air-gapped industrial control systems in nuclear power plants uses Metasploit to execute pre-built Modbus/TCP attack modules against the user interface and controller, while Ettercap performs man-in-the-middle attacks in the same ICS TB to generate malicious traffic for training and validating the detection model [180]. A SCADA security study on covert penetrations of Modbus-based systems employs Ettercap to carry out Address Resolution Protocol (ARP)-poisoning attacks, enabling stealthy hijacking and blackout scenarios in a SCADA environment and producing traces that illustrate how protocol-level weaknesses can be exploited while remaining difficult to detect [196]. An industrial control CR built on VMware virtual machines uses Metasploit as the main penetration-testing framework: after deploying several target machines, a Kali Linux attacker host runs Metasploit to exploit vulnerable services on the industrial network, supporting hands-on training and vulnerability assessment in the emulated ICS environment [100].

Attack strategy and support

A virtual wastewater treatment ICS environment uses MITRE ATT&CK as a threat-emulation tool to structure and execute adversary behaviour against specific industrial automation levels, allowing the impacts of Modbus/TCP protocol attacks on the process to be analysed systematically [101]. The Tectonic academic CR adopts MITRE ATT&CK as the basis for building threat models and rule sets, so that attack rules can be extended with techniques, tactics, and procedures from the framework and used to recognise student behaviours in automated training scenarios [64]. In an emulated industrial-control TB, iptables is configured for traffic redirection, rerouting communication that would normally flow between the HMI and PLC so that it instead passes through an attacker host for cyber-threat experimentation in realistic ICS scenarios [52]. A 5G/6G security dataset generation framework uses iptables in a man-in-the-middle scenario by adding forwarding rules on the attacker entity, enabling interception and manipulation of traffic when constructing IP-layer and

core-network persistent Protocol Data Unit (PDU) session attack traces [10].

Denial of Service & Distributed Denial of Service

An IoT forensics TB for cyberattack attribution uses Hping and scapy as traffic-generation tools to create TCP SYN flood and SMURF attack traffic in an IoT/IIoT network, producing malicious traces that are included in the IoT-CAD dataset for attribution experiments [109]. In a cooperative smart-farming security study, Hping is used as a denial-of-service tool to launch TCP SYN flood attacks against smart-farming and digital-twin components, supporting the creation of datasets that capture threats to agricultural edge and digital-twin architectures [132]. A HiL TB simulating renewable-energy plants relies on scapy as a network-interaction library to construct, dissect, and manipulate S7 protocol packets, enabling detailed control and modification of industrial control traffic when analysing data-modification attacks in power-system cybersecurity experiments [79].

Packet Manipulation

A federated transfer-learning study for network anomaly detection uses Ettercap as a packet-manipulation tool to conduct ARP-poisoning attacks from a Kali Linux attacker host, generating manipulated traffic for evaluating the proposed defence approach [133]. In a digital power-twin environment for power-system cybersecurity, Ettercap is integrated into the attack designer and launcher components, where its API is used to perform man-in-the-middle attacks through targeted packet manipulation against the emulated power-system communication [74]. A HiL TB targeting attacks on the Siemens S7 protocol employs scapy as a packet-manipulation framework, using attack scripts that define, dissect, and construct S7 communication frames for detailed network interaction during ICS attack experiments [79]. The SCASS modular SCADA security TB uses scapy to implement false-data injection (FDI) attacks by crafting and injecting modified protocol messages, enabling systematic study of FDI attack techniques in industrial-control environments [44].

Vulnerability Management

A cyber exercise platform that compares container-based virtualization with other deployment options uses Owasp Zap (Zed Attack Proxy) and SkipFish as web-application vulnerability scanners. Each server is prepared as a vulnerable environment, and both tools are used to scan the hosted web applications for vulnerabilities, allowing the study to compare their behaviour across different physical and virtual setups [117]. An open-source platform for analysing commercial IoT devices employs Owasp Zap (Zed Attack Proxy) and SkipFish to gather information and scan for vulnerabilities in web interfaces exposed by the devices. The tools are run before the main experiments to search for device vulnerabilities and related exploit attempts, supporting systematic security assessment of the connected devices [2].

Password Cracking & Credential Harvesting

A CR scenario framework uses Hydra as a password-cracking tool to let a red team simulate attacks that attempt to recover a manager's password using the rockyou wordlist, integrating credential-attacks into scripted scenario execution within the CRACK environment [150]. The IoT-CAD digital-forensics TB employs Hydra as a password-attack tool that targets an admin account on a selected host using a wordlist generated earlier in the workflow, producing credential-attack traffic for AI-based cyberattack-attribution experiments in IoT environments [109]. A log-data generation TB for cybersecurity experiments uses Mimikatz as a credential-harvesting tool in adversary-emulation scenarios, where typical attacker steps are implemented with common security tools so that realistic host and network logs can be recorded for intrusion-detection research [188]. A cyber exercise on the EPIC microgrid TB integrates Mimikatz as a credential-dumping tool to perform credential-oriented operations against SCADA and firewall components, enabling trainees to observe and respond to credential-compromise scenarios in a power-systems context [96].

Brute Force Attacks

An IoT/IIoT TB architecture for evaluating AI-based security systems at the edge uses Hydra and Cewl as brute-force attack tools. Cewl, classified as a tool for wordlist generation in brute-force attacks, is combined with Hydra, a password-cracking tool, to launch automated password-hacking scenarios against vulnerable nodes in the TB, producing realistic credential-attack data for the TON_IoT datasets [111]. In the IoT-CAD digital-forensics TB, Cewl again serves as a wordlist-generation tool by crawling website content to build custom password lists, while Hydra is used as a password-attack tool that tests the admin account against this generated wordlist. Together, they implement brute-force password attacks that generate malicious traffic for evaluating cyberattack-attribution methods in IoT environments [109].

Adversary Emulation

A TB for APT research uses MITRE Caldera as an adversary-emulation tool to run APT campaigns, exploiting its scalability and adaptability to generate realistic attack activity for building a comprehensive APT dataset and supporting the development of robust defences [174]. The Tectonic academic CR integrates MITRE Caldera as a tool to automate attacks in training scenarios, where it is combined with monitoring services so instructors can evaluate student performance while Caldera drives configurable attack campaigns within the CR environment [64]. Infection Monkey is employed as an adversary-emulation tool for attack and breach simulation in a framework for automating security scenarios, where it acts as one of the applications that provide red-team capabilities in order to test and improve organisational security readiness against real-world cyber attacks [3].

Phishing and Social Engineering
A Docker-based Android platform for mobile-focused CRs uses Gophish as a phishing campaign simulation tool. Gophish is integrated as a web application that crafts and sends phishing emails, with a Dockerized version included in the framework to support phishing and social-engineering exercises for mobile devices [30]. A case study on mitigating injection and phishing attacks employs ZPhisher as a phishing and social-engineering tool to create phishing websites. These phishing sites are used in experiments that analyse security attacks associated with injection and phishing and evaluate how inspection plugins can help implement a more secure environment [23].
Reverse Engineering and Binary Analysis
An automated IoT security TB integrates Binwalk as a reverse-engineering tool for firmware threat and vulnerability assessment, where device firmware is inspected to identify outdated and therefore potentially vulnerable versions. In the same TB, Dex2jar is used as a reverse-engineering tool for mobile applications to disassemble Android apps and check whether they contain hard-coded credentials, which are treated as a sign of vulnerability. Both tools are part of an open-source platform designed to analyse commercial IoT devices and detect attacks against them [2].
Proxy and Web Interception
A wastewater treatment ICS security study uses Ettercap as a proxy and web interception tool to perform integrity attacks by intercepting and manipulating communication in the industrial control network, evaluating standalone and hybrid SDN-based defences against channel attacks in a wastewater treatment plant (WWTP) case study [102]. A multicast network security TB employs Owasp Zap (Zed Attack Proxy) as a proxy and web interception tool to generate malicious web traffic and to specify attack URLs via its browser plug-in, enabling the performance evaluation of firewalls and security mechanisms under different attack and network configurations [187] (Table 1).

4.3.2 Data storage

Databases and other data storage technologies are reported across all CR and TB *application areas*, but only a small number of publications describe them explicitly. Figure 9 quantifies coverage by *application area* and subdomain. ICT shows the highest overall activity with 12 mentions, followed by Power Systems (5) and RAN & Mobile Devices (5). IoT/IIoT accounts for 4 mentions, while CPS (3) and ICS (3) are less frequent. Intelligent Transportation Systems remains sparse with 2 mentions. Across subdomains, Relational Database remains the most common with 15 mentions, concentrated in ICT (7) and present in Power Systems (3), ICS (2), CPS (1), IoT/IIoT (1), and Intelligent Transportation Systems (1). NoSQL Database totals 9, led by ICT (3) and RAN & Mobile Devices (3), with additional entries in Power Systems (1), IoT/IIoT (1), and Intelligent Transportation Systems (1). Time series database appears 5 times, distributed across RAN & Mobile Devices (2) and CPS, ICS, and Power Systems (1 each). Storage backends beyond databases are rare. File & Block Storage occurs only in IoT/IIoT (2). Object Storage is reported in ICT (1) and CPS (1). Event and Log Storage appears once in ICT (1). Overall, Figure 9 indicates that data storage in CRs and TBs is mainly based on databases, with relational databases most common and NoSQL databases second, while other storage components are reported only selectively. In some publications, the primary application of databases is mentioned as the target system for cyberattacks in various scenarios, as described in Chapter 4.3.1.
Relational Database
A smart-airport IIoT cyber TB uses a MySQL database as a relational backend for long-term storage of labelled network flows and telemetry, providing the main data repository for IIoT cyber-twin attack and defence scenarios in the SAIR-IIoT environment [84]. A smart-grid CR generation framework relies on a MySQL database as an open-source relational store that connects virtual IEDs with the power-system simulator, enabling automated creation and management of smart-grid CR instances from power-system models [106]. In an information-environment operations TB, PostgreSQL is used as the relational database of the core server and is accessed via a FastAPI REST interface. Grafana dashboards are integrated on top. PostgreSQL was selected because it is natively supported by Grafana [185]. The ICSSIM industrial-control simulation framework uses SQLite as a shared relational database file between Docker containers so that simulated ICS components can access common data, supporting integrated testing of industrial-control scenarios [47].
NoSQL Database
A real-time EV ecosystem cybersecurity monitoring architecture uses MongoDB as a Not Only SQL (NoSQL) database to store charging-session command histories and telemetry collected from multiple Simple Network Management Protocol (SNMP) agents, providing the persistent backend for analysing EV data and detecting cyberattacks [146]. A framework for generating full-stack 5G and 6G security datasets relies on MongoDB as a NoSQL store for network registration data, which is queried by core-network functions when reconstructing persistent PDU sessions for IP-layer and core-network attack scenarios [10]. In a cooperative smart-farming security study, an AWS NoSQL DB is used as the cloud data store for sensor readings, enabling farms to access sensor data according to authorisation policies and supporting the training and evaluation of a lightweight edge convolutional neural network (CNN)–Transformer model on smart-farming and digital-twin attack datasets [132].

Table 1 Top-10 Technologies per Subdomain for Red Team Operations. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Adversary emulation	5	2	MITRE Caldera (4), Infection Monkey (1)	ICS, ICT
Attack Strategy & Support	26	20	MITRE ATT&CK (6), Iptables/nftables (2), ABB Robot Studio (1), Avet (1), Cyber Kill Chain (CKC) (1), Freesweep (1), Microsoft Threat Modelling Tool (1), Nginx Web server (1), Node-RED (1), OpenSSH (1)	ICS, ICT, IoT, IIoT, RAN & Mobile Devices
Brute force attacks	9	5	Hydra (4), Cewl (2), DirBuster (1), Dirb (1), Medusa (1)	CPS, ICS, ICT, IoT, IIoT, RAN & Mobile Devices
Denial of Service & Distributed Denial of Service	29	14	Hping (12), scapy (4), Slowhttptest (2), Coin Hive (1), Geth (1), HULK (1), Memtester (1), Metasploit (1), Mirai (1), Slowloris (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems
Exploitation and Attack Execution	58	18	Metasploit (23), Ettercap (8), Sqlmap (6), Arpspoof (3), Bettercap (3), Airgeddon (2), SSLStrip (2), Burp (1), DEEP EXPLOIT (1), Mimikatz (1)	ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Network Scanning and Reconnaissance	61	17	Nmap (31), Wireshark (7), MulVAL (3), Netdiscover (3), Xprobe2 (3), Shodan (2), scapy (2), Ettercap (1), Hping (1), Nessus (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Paketmanipulation	16	6	scapy (6), Ettercap (5), Arpspoof (2), Wireshark (1), aireplay-ng (1), dsniff (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Password Cracking and Credential Harvesting	11	4	Hydra (7), Mimikatz (2), John The Ripper (1), LaZagne (1)	ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Phishing and Social Engineering	2	2	Gophish (1), ZPhisher (1)	ICT, RAN & Mobile Devices
Proxy and Web Interception	2	2	Ettercap (1), Owasp Zap (Zed Attack Proxy) (1)	ICS, ICT
Reverse Engineering and Binary Analysis	4	4	Binwalk (1), Dex2jar (1), Ghidra (1), Immunity Debugger (1)	ICT, IoT, IIoT, RAN & Mobile Devices
Training and Practice Systems	50	26	Apache web server (5), DVWA (5), MySQL Database (5), CTFd (4), Metasploitable (4), LAMP stack (3), Wordpress (3), Mosquitto MQTT Broker (2), OWASP Juice Shop* (2), CURA (1)	ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Vulnerability Management	14	11	Owasp Zap (Zed Attack Proxy) (2), SkipFish (2), sFuzz (2), InsightVM (1), LinPEAS (1), Nikto (1), Nmap (1), OpenVAS (1), Wascan (1), scapy (1)	ICT, Intelligent Transportation Systems, IoT, IIoT, RAN & Mobile Devices

Time-series database

A cyber-physical security TB for a multi-stage manufacturing system uses InfluxDB as a time-series database to collect continuous process and sensor data alongside traditional cyber-monitoring information, providing a unified real-time data store for analysing physical and cyber events in the manufacturing environment [41]. An open O-RAN TB with AI-enabled control and monitoring employs InfluxDB as a time-series backend for iPerf and latency measurements, storing real-time metrics that support anomaly detection and performance analysis in the radio-access network [129]. PingThings' Berkeley Tree Database (BTrDB) is used as a high-performance time-series database in the RT-METER multi-layer cyber–power TB, storing sensor and communication-network data so that real-time power-grid

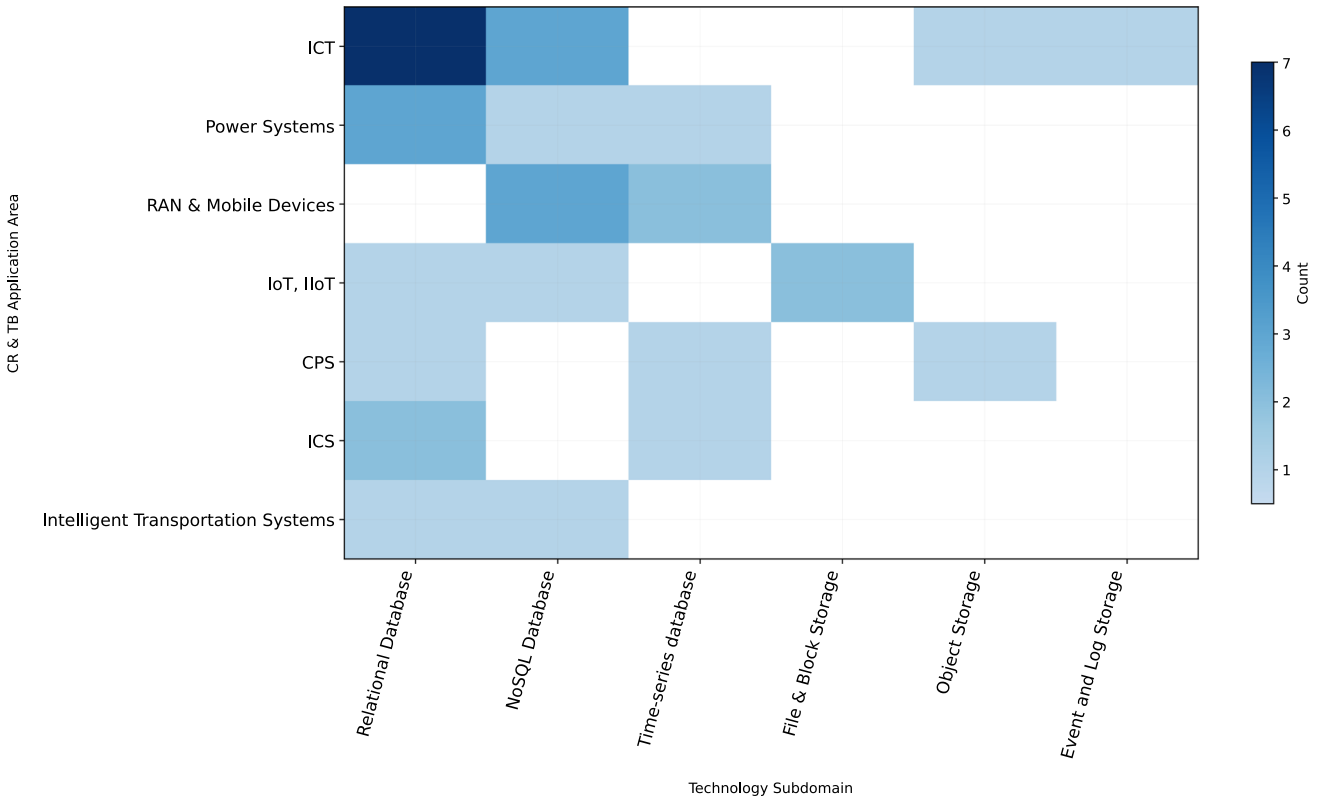


Fig. 9 Data Storage Subdomain Distribution Across Cyber Range Application Areas

resilience analyses can be performed across both physical and cyber layers [116].

File and Block Storage

A blockchain-based security framework for IoT maritime transportation systems uses InterPlanetary File System (IPFS) as a distributed file and block storage system to store sensor data collected by edge servers in an IoT/IIoT setting [92]. IPFS Kubo is used in the same framework as the implementation tool for deploying and operating this IPFS-based storage layer, providing the underlying distributed storage infrastructure for the recorded sensor data [92].

Object Storage

A secure edge-computing reference architecture for data-driven structural health monitoring uses AWS Simple Storage Service (S3) as an object-storage service for Technical Data Management Streaming (TDMS) files, where Raspberry Pi edge devices send measurement data via AWS IoT Greengrass to S3 for persistent storage and later analysis [59].

Event and Log Storage

In a TB for APT, Elasticsearch is used as part of an Elasticsearch, Logstash, and Kibana (ELK)-based monitoring box that provides real-time storage, analysis, and visualization of event logs, supporting the collection of telemetry from multiple APT scenarios to study attacks and develop robust defences [174] (Table 2).

4.3.3 Monitoring and analytics

This *technology domain* covers monitoring and analytics technologies used across CRs and TBs. Figure 10 quantifies coverage by domain and subdomain. ICT shows the highest overall activity with 67 mentions, followed by ICS (27), IoT/IIoT (19), Power Systems (17), RAN & Mobile Devices (16), CPS (11), and Intelligent Transportation Systems (6). Across subdomains, Analysis & Verification leads with 54 mentions, followed by Data Collection (43), Log Management (32), and Visualization & Dashboarding (30). Assets Monitoring is rare with only 4 mentions. Within Analysis & Verification, activity is concentrated in ICT (16) and ICS (11), with additional use in RAN & Mobile Devices (7), Power Systems (6), Intelligent Transportation Systems (6), CPS (5), and IoT/IIoT (3). Data Collection is led by ICT (15) and IoT/IIoT (11), followed by ICS (8), Power Systems (5), and CPS and RAN & Mobile Devices (2 each). Log Management is dominated by ICT (19) with further entries in ICS (5), Power Systems (4), and RAN & Mobile Devices (4). Visualization & Dashboarding peaks in ICT (15) and appears in CPS (4), ICS (3), IoT/IIoT (3), RAN & Mobile Devices (3), and Power Systems (2). Assets Monitoring is reported only in ICT (3) and IoT/IIoT (1). Overall, monitoring and analytics in CRs and TBs are driven by analysis and data-collection workflows, with ICT contributing the broad-

Table 2 Top-10 Technologies per Subdomain for Data Storage. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Event and Log Storage	1	1	Elasticsearch† (1)	ICT
File & Block Storage	2	2	IPFS* (1), Ipfs Kubo† (1)	IoT, IIoT
NoSQL Database	9	6	MongoDB† (4), AWS NoSQL DB† (1), Amazon DynamoDB* (1), Elasticsearch† (1), NoSQL database* (1), Redis database† (1)	ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Object Storage	2	1	AWS S3*† (2)	CPS, ICT
Relational Database	15	5	MySQL Database*† (8), SQLite*† (3), PostgreSQL† (2), MariaDB† (1), Microsoft SQL Database* (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems
Time-series database	5	2	InfluxDB† (4), PingThings' Berkeley Tree Database (BTrDB)† (1)	CPS, ICS, Power Systems, RAN & Mobile Devices

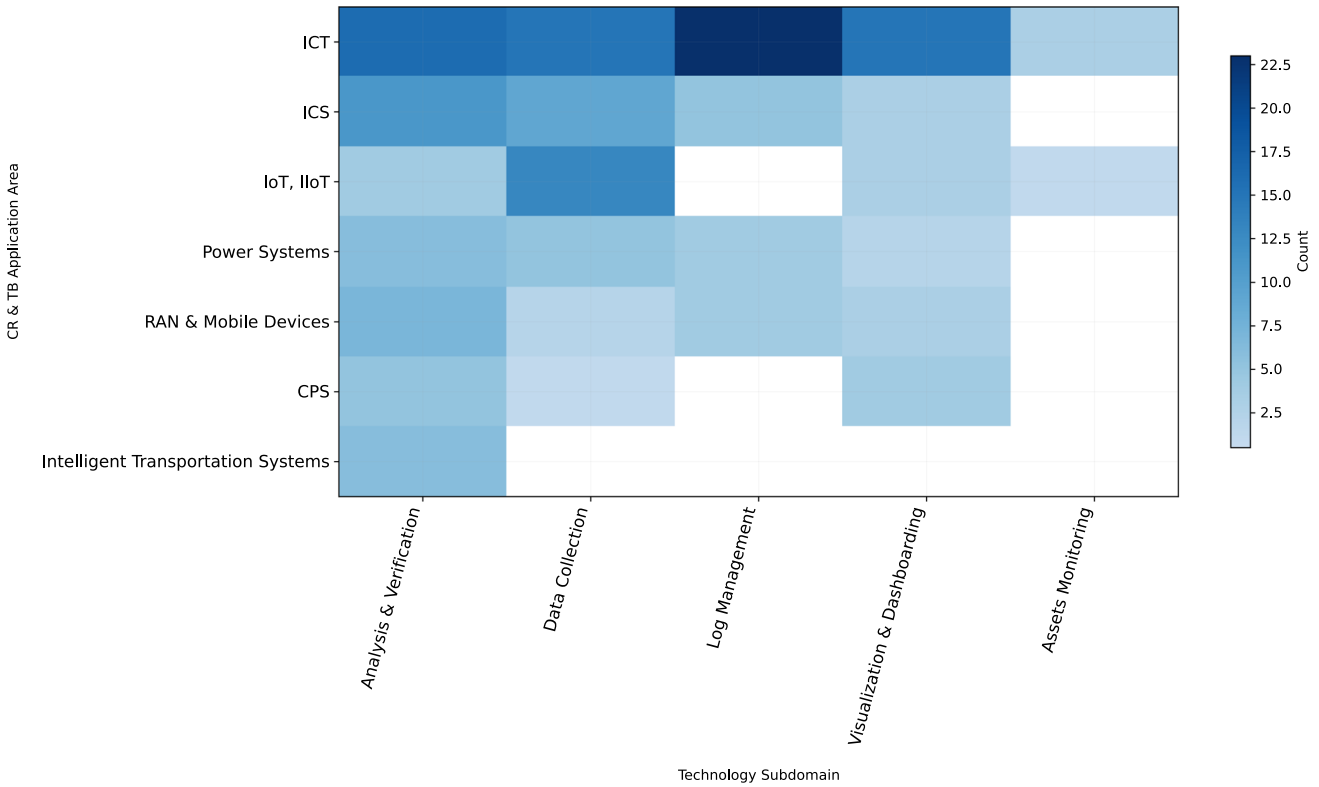


Fig. 10 Monitoring and Analytics Subdomain Distribution Across Cyber Range Application Areas

est and deepest coverage, while assets-oriented monitoring remains comparatively uncommon.

Analysis and Verification

In a cyber-physical security TB for a multi-stage manufacturing system, Wireshark is used for network traffic capture and analysis by logging network traffic, extending monitoring beyond traditional cyber data to include sensor data alongside other TB components [41]. In a penetration-testing TB for 5G systems, Wireshark is used for live traffic capturing and feature extraction by analysing traffic on individual network segments in simulated topologies, supporting the execution and analysis of attacks in the designed environment [34]. A Modbus-focused SCADA security study uses ScadaBR as the SCADA control-centre HMI on a dedicated virtual machine, where it communicates with a Modbus server to support covert SCADA hijacking and blackout attack scenarios that exploit protocol weaknesses [196]. In a smart-grid Cyber Range as a Service on an OpenStack cloud platform,

ScadaBR functions as the SCADA system on the substation host within a virtual environment that imitates real system infrastructure and supports automated instantiation and use of smart-grid cyber-range instances [35].

Data Collection

Wireshark is used for network dataset generation in a cooperative smart-farming security study, where it monitors wireless access points and records traffic to identify access points and list their basic service set identifiers (basic service set identifiers (BSSIDs)) as part of building smart-farming network datasets for threat analysis [132]. In a 5G security study on HTTP/2 anomaly detection, Wireshark serves as a packet-capture tool in the data-collection process, recording HTTP/2 packets during normal operation of the 5G network to provide input traces for the proposed anomaly-detection framework [200]. Tcpdump is used in a flexible hybrid TB for securing industrial systems, where raw inbound and outbound network traffic is captured and stored as part of a comprehensive logging setup that collects all possible logs from the TB to support cyber-defence evaluation and subsequent traffic analysis [43]. In a substation-focused cybersecurity dataset, Tcpdump is employed to capture network traffic over a seven-day period using embedded software, collecting packet traces that are later used to train intrusion-detection systems based on machine-learning models for electrical substations [65].

Log Management

In the DefAtt architecture of virtual cyber labs for research and education, Elastic Logstash is used for event data processing and filtering by enriching shipped events with filters to modify or annotate them, while Elasticsearch provides real-time search and analysis of logs by storing the data as documents in one or more indices within the DefAtt environment that focuses on network-based attacks and their defences [104]. A TB for reproducible and adaptable log data generation for cybersecurity experiments uses Elastic Logstash and Elasticsearch together for log data storage and search: Elastic Logstash is responsible for collecting, storing, searching, and visualizing log data, and Elasticsearch supports log data collection, storage, search, and visualization in a TB designed to generate realistic log data for sound cybersecurity experiments [188].

Visualization & Dashboarding

A railway infrastructure security and resilience simulation TB uses Grafana as a presentation dashboard, where several analysis tools and a Grafana-based dashboard were developed to display information from running experiments, including DDoS attack scenarios [119]. In a cooperative smart-farming infrastructure, Grafana is installed at each farm as a visualization tool to provide a more intuitive and detailed representation of the sensor data used in the efficient federated transfer learning-based anomaly detection setup [133]. A TB for APT employs Kibana as part of an ELK-based monitoring box that combines Elasticsearch, Logstash, and Kibana to provide real-time storage, analysis, and visualization of event logs collected from multiple APT scenarios [174]. In a TB focused on generating realistic log data for cybersecurity experiments, Kibana is used on the log server as a visualization tool to analyse the generated log datasets directly before they are optionally exported for offline use [188].

Assets Monitoring

In an open-source CR designed to strengthen cybersecurity learning, Prometheus is used as a monitoring tool to provide monitoring services together with Moodle and Grafana in the deployment, supporting improved educational outcomes and monitoring within the range [37]. Within the SEA-Guard framework for IoT maritime transportation systems, Prometheus is deployed alongside the blockchain platform to collect performance metrics that are then visualized with the monitoring components, enabling observation of the behaviour and performance of the proposed architecture [92] (Table 3).

4.3.4 Computing platform

This *technology domain* covers computing platform technologies that underpin CRs and TBs. Figure 11 quantifies coverage by *application area* and subdomain. ICT dominates overall with 101 mentions, followed by ICS (30), Power Systems (16), IoT/IIoT (14), RAN & Mobile Devices (13), CPS (10), and Intelligent Transportation Systems (6). Across subdomains, Cloud Infrastructure (35) and Containerisation (35) are jointly the most frequently reported. They are followed by Infrastructure Provisioning and Configuration (28), Virtualization platform/Type-2-Hypervisor (24), Virtualization platform/Type-1-Hypervisor (21), Integrated Testbed Solutions (14), Software Provisioning and Configuration (13), Container Orchestration (9), Integrated Cyber Range Solutions (8), and Infrastructure Instantiation Systems (3). At the *application area* level, Containerisation is concentrated in ICT (13) and ICS (10), with additional use in RAN & Mobile Devices (6). Cloud Infrastructure is led by ICT (18) and appears consistently in ICS, Power Systems, and IoT/IIoT (4 each). Infrastructure Provisioning and Configuration peaks in ICT (23) and occurs only sporadically in the other *application areas*, while it is not reported for ICS. Virtualization technologies are mainly reported for ICT and ICS, with Type-2 hypervisors at 12 in ICT and 6 in ICS, and Type-1 hypervisors at 9 in ICT and 6 in ICS. Software Provisioning and Configuration is almost entirely concentrated in ICT (11) and appears only marginally in Power Systems (2). Integrated Testbed Solutions are distributed across all *application areas* with small counts, and Container Orchestration is mainly reported in ICT (4) and RAN & Mobile Devices (3). Overall, computing platform coverage is driven by ICT-focused use of cloud and container based stacks, supported by virtualization, while

Table 3 Top-10 Technologies per Subdomain for Monitoring and Analytics. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Analysis & Verification	55	34	Wireshark† (12), ScadaBR*† (4), Tshark† (4), Zeek† (2), iPerf† (2), osquery† (2), sFlow† (2), 5g-trace-visualizer† (1), Afra† (1), Apache JMeter† (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Assets Monitoring	4	1	Prometheus† (4)	ICT, IoT, IIoT
Data Collection	45	22	Wireshark† (13), Tcpdump† (6), scapy† (3), CICFlowMeter† (2), Packetbeat† (2), Tcpreplay† (2), Tshark† (2), Apache Flume† (1), Apache Kafka† (1), Elastic Agent† (1)	ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Log Management	36	21	Elasticsearch† (6), Elastic Logstash† (4), rsyslog† (3), ELK Stack† (2), Elastic Beats† (2), Winlogbeat† (2), AWS CloudTrail* (1), AWS X-Ray* (1), Amazon CloudWatch* (1), CSV† (1)	ICS, ICT, Power Systems, RAN & Mobile Devices
Visualization & Dashboarding	30	16	Kibana† (9), Grafana† (6), Matplotlib† (2), AWS Grafana† (1), AWS QuickSight† (1), EasyBuilder† (1), FUXA† (1), Gephi† (1), MLFlow† (1), Node-RED* (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems

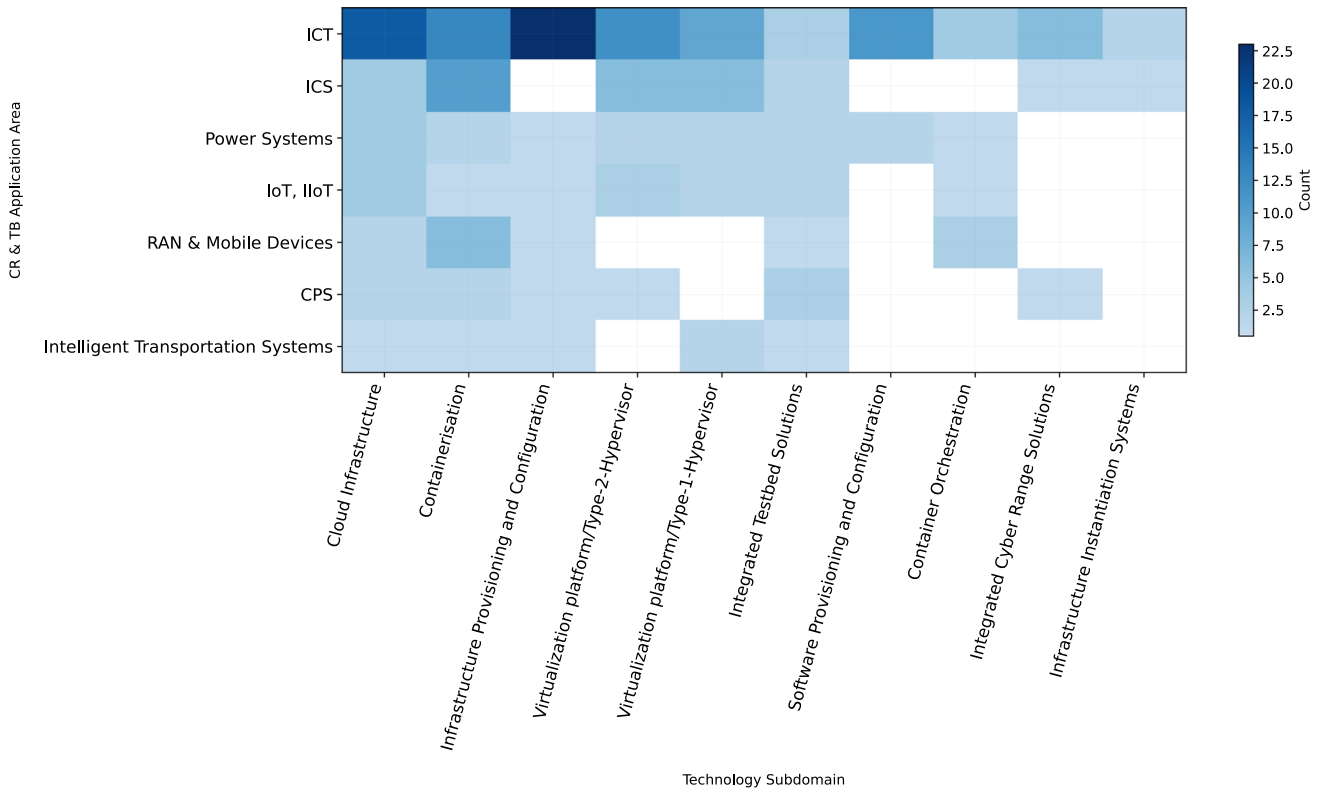


Fig. 11 Computing Platform Subdomain Distribution Across Cyber Range Application Areas

integrated solutions and automated instantiation mechanisms are reported less frequently across the *application areas*.

Cloud Infrastructures

An autonomous cybersecurity TB for OT networks uses OpenStack as a tool for dynamic control over the compute, storage, and network resources needed for digital twin instantiation, by providing an easy-to-deploy OpenStack-based network emulator used to test various attack types that lead to OT plant instability [140]. A CR for scalable cybersecurity experiments and training uses OpenStack as cloud computing infrastructure: the NCL offers a cloud computing environment with a prototype implementation on top of the OpenStack infrastructure, so that the CR, a virtual environment imitating critical infrastructure, can be deployed on an OpenStack cloud platform [35]. An AWS Elastic Compute Cloud (EC2) public cloud CR deployment uses AWS as a platform for CR cloud deployment, introducing an approach that runs cybersecurity training activities on the AWS cloud at scale and at relatively low cost [19]. An IIoT security TB for assessing and mitigating network vulnerabilities uses AWS as cloud IoT infrastructure, where sensors with different protocols send data via monitoring gateways that forward the data to the AWS cloud through a DMZ to study operational and cybersecurity risks associated with IIoT deployments [75].

Containerisation

A cyber-physical fuzzing framework for unmanned aerial vehicle (UAV) systems configures its simulation environment on an Ubuntu Linux host where Docker provides the containerised runtime for the flight-behaviour simulations that are exercised and analysed for butterfly-effect phenomena in the UAV control loop [90]. In the ICSSIM framework for building ICS security TBs, each ICS component is simulated inside an isolated Docker container so that modules can be flexibly combined, extended, or replaced when constructing custom ICS security experiments [47]. The MaCySTe virtual maritime TB, which reproduces the network infrastructure and core components of onboard cyber–physical systems for realistic cybersecurity testing and training with maritime operators, starts each training scenario via shell scripts that rely on Podman to create container networks and execute pods and Flatpak-based applications [99].

Infrastructure Provisioning and Configuration

A large-scale CR for cybersecurity training uses Terraform as an infrastructure-as-code workflow engine together with VMware vSphere to create and store virtual machine (VM) templates, including components such as Active Directory, domain name system (DNS), and domain controllers, enabling the range infrastructure to be deployed in a versatile way with minimal manual work [126]. In the Tectonic academic CR, Terraform is used for automated infrastructure deployment by defining the resources to be instantiated and the configurations to be applied, while Libvirt provides on-premises virtualization that instructors use to deploy systems and networks for the training scenarios [64]. For the CryptoGuard cryptojacking study, Libvirt is employed to run multiple VMs on a host in order to establish the TB for data collection, enabling experiments to be performed on several VMs under a common setup [130]. In the CyberExpert experiential learning platform, Libvirt serves as the virtualization API that tools such as Foreman and Guacamole use to control and start VMs, supporting a virtual and hands-on CR environment for higher-level cybersecurity training [66].

Virtualization platform/Type-2-Hypervisor

A virtual cyber lab platform for network-based attack and defence training uses VirtualBox as a virtualization platform (Type-2 hypervisor) to simulate machines in a networked environment as VMs, enabling CR lab environments to be created and deployed for education and research with minimal cost [104]. In a smart-grid cybersecurity TB, VirtualBox is used for substation and control-centre simulation by running VMs that replicate hardware at both locations, with the virtualized network connected through a router VM in order to emulate the smart-grid communication environment [214]. An industrial-control CR for security training is based on VMware Workstation as the virtualization platform, which manages all VMs and controls operations such as startup, suspension, and shutdown of the operating systems used in the training scenarios [100]. The IoT-CAD digital-forensics TB employs VMware Workstation to host the VMs in the application layer, including a Kali Linux VM that acts as an offensive system to execute attacks against IoT devices and services for cyberattack-attribution experiments [109].

Virtualization platform/Type-1-Hypervisor

A study on time-based virtual machine migration as a moving target defense against host-based attacks models attacker and victim machines as VMs running on the Kernel-based Virtual Machine (KVM) hypervisor, where both VMs run Ubuntu Server 20.04.2 with kernel 5.4.0–72 and KVM 4.2.1, so that KVM provides the virtual machine management layer for the Stochastic Petri Net–based evaluation environment [183]. In the PenGym framework for training reinforcement-learning penetration-testing agents, KVM is used for virtual machine management as the virtualization technology that underpins the CR, enabling the creation of VMs with predefined services and processes as part of the network environment used for realistic agent training [121]. A large-scale CR for cybersecurity training uses VMware vSphere as a computing platform to create and store VM templates, where vSphere is employed to build and manage templates that include components such as Active Directory, DNS, and domain controllers as part of a flexible training infrastructure [126]. In a real-time monitoring architecture for enhanced cybersecurity in the EV ecosystem, vSphere is described as a computing platform used to manage and deploy the VMs that host the components of the EV monitoring framework, supporting the collection

and analysis of data from different EV ecosystem elements [146].

Integrated Testbed Solutions

A real-time cyber-physical simulation TB for large-scale power systems uses EXata CPS (Cyber-Physical Network Simulator) to simulate the cyber network: EXata network modelling is used to model the cyber system and interact with the real-time network emulation that runs on the EXata server, while real-time simulators from OPAL-RT and RTDS simulate the power grids [123]. An experimental TB on security and stability challenges in inverter-based solar distributed generation systems incorporates EXata CPS as cyber network simulation software to simulate the cyber network, supporting various industrial protocols and technologies and allowing the simulation of complex network scenarios whose vulnerabilities and potential impacts are analysed [115]. Aerial Experimentation and Research Platform for Advanced Wireless (AERPAW) is used as drone infrastructure in a TB that explores optimization methods for federated learning-enabled network incident anomaly detection in drone swarms, evaluating defence mechanisms such as differential privacy and adversarial training and collecting accuracy, system, and network usage metrics under test cases including benign, mildly poisoned, highly malicious, and safe situations [85].

Software Provisioning and Configuration

In a large-scale CR for cybersecurity training, Ansible is used as a configuration management engine for software provisioning, helping to deploy the range infrastructure in a versatile and flexible way with minimal manual work [126]. A cloud-based smart grid CR for scalable cybersecurity experiments and training uses Ansible on the controller host to automate the provisioning of controller and substation nodes as part of the virtual environment on an OpenStack cloud platform [35]. In work on APT scenarios for CRs, AWX is used as administration software for APT scenario administration and orchestration, where a graph-based logic engine for APT scenarios is operated in combination with AWX in fully virtualized CRs [21].

Container Orchestration

A cryptojacking defence framework for Linux cloud environments uses Kubernetes for container orchestration by deploying the CryptoGuard agent as a DaemonSet so that a monitoring pod runs on every node and can collect syscall data across the whole cluster [130]. In a 5G core anomaly-detection setup, all 5G core network functions are deployed as Kubernetes pods using Helm charts from a public repository, so that the 5GCGuard framework runs on a Kubernetes-managed 5G core environment for evaluating anomaly detection [177]. A Raspberry-Pi-based CR for web-attack training uses Docker Swarm as the container-orchestration platform to automatically distribute new containers across different cluster nodes for load balancing and to manage the cluster nodes wirelessly [125]. In a smart-grid Cyber Range as a Service, a deployment tool builds Docker images on each node and starts Docker Swarm overlay networks so that the CR, realised as a virtual environment on an OpenStack cloud platform, can orchestrate containers across the participating nodes [35].

Integrated Cyber Range Solutions

A study on comparing reproduced cyber experimentation across different emulation TBs uses Minimega as an emulation-based cyber TB, where a mathematical model is validated against experiments using the Minimega emulation and lessons are drawn on the reproducibility of the original experiments and the detection of adversary network scanning using emulation [178]. In work on the verification of cyber emulation experiments through virtual machine and host metrics, Minimega is used as an emulation platform: the framework instantiates Minimega to evaluate Iceberg CRX and to support the evaluation of exercises in this emulation-based environment [181]. The GeNIS network-intrusion dataset is developed using the cloud-based network simulation infrastructure that GECAD has available on the Airbus CyberRange platform, where the platform provides the resources for generating traffic and raw network packets in an enterprise topology that includes malicious flows from attackers, benign traffic from legitimate users, and background traffic of an enterprise computer network [166].

Infrastructure Instantiation Systems

A CR platform for training uses Naumachia as an infrastructure instantiation system for infrastructure provisioning and configuration. Naumachia is described as a Docker network designed to give each challenge an isolated environment, deployed as a distinct Docker container, within a platform built from open-source tools for topics such as Snort ruling, forensic analysis, and man-in-the-middle spoofing [192]. A cloud-based CR deployment extends the functionality of the CR instantiation system Cyber Range Instantiation System (CyRIS), which is available as open source on GitHub, to realise an approach that uses the AWS EC2 public cloud platform to run cybersecurity training activities at scale and at relatively low cost [19]. In the PenGym framework for training penetration testing agents, CyRIS provides an automatic CR creation mechanism. The Action/State Module acts as an interface between agents and the environment, and this automatic CR creation mechanism is integrated into PenGym by leveraging CyRIS to support network environment creation and good execution performance [121] (Table 4).

4.3.5 Custom development

This *technology domain* covers custom development technologies used in CRs and TBs. Figure 12 shows coverage by *application area* and *technology subdomain*. ICT concentrates most activity with 70 mentions, followed by IoT, IIoT

Table 4 Top-10 Technologies per Subdomain for Computing Platform. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Cloud Infrastructure	33	9	OpenStack* (18), Amazon Web Services (AWS)* (7), Google Cloud* (2), Azure Digital Twins* (1), DevStack* (1), DigitalOcean VPC* (1), GENI cloud* (1), Microsoft Azure* (1), Skytap* (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Container Orchestration	9	4	Kubernetes‡ (4), Docker Swarm‡ (2), Helm*‡ (2), Rancher‡ (1)	ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Containerisation	35	2	Docker* (34), Podman‡ (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Infrastructure Instantiation Systems	3	2	CyRIS*‡ (2), Naumachia‡ (1)	ICS, ICT
Infrastructure Provisioning and Configuration	28	15	Terraform‡ (7), Libvirt‡ (4), Packer‡ (4), Vagrant‡ (2), Apache ARIA‡ (1), Boto3‡ (1), Clonezilla* (1), Docker Hub‡ (1), Flatpak‡ (1), Foreman‡ (1)	CPS, ICT, IoT, IIoT
Integrated Cyber Range Solutions	8	7	Minimega*‡ (2), Airbus CyberRange* (1), CyTrONE* (1), DIATEAM's Hybrid Network Simulation (HNS) cyber range platform* (1), EDURange* (1), KYPO* (1), Norwegian Cyber Range* (1)	CPS, ICS, ICT
Integrated Testbed Solutions	14	13	EXata CPS (Cyber-Physical Network Simulator)* (2), AERPAW (Aerial Experimentation and Research Platform for Advanced Wireless)* (1), CyberVAN* (1), DETERLab* (1), FIT IoT-LAB* (1), ICSSIM Framework* (1), Microsoft CyberBattleSim* (1), NSF POWDER Wireless platform* (1), PASTA (Portable Automotive Security Testbed with Adaptability)* (1), SAir-IIoT Cyber Testbed* (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Software Provisioning and Configuration	13	2	Ansible‡ (12), AWX‡ (1)	ICT, Power Systems
Virtualization platform/Type-1-Hypervisor	21	5	VMWare vSphere* (9), KVM* (5), Proxmox VE* (4), VMWare ESXi* (2), Microsoft Hyper-V* (1)	ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems
Virtualization platform/Type-2-Hypervisor	24	5	VirtualBox* (11), VMWare Workstation* (6), QEMU* (3), VMWare* (3), QEMU-IOL* (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems

(21), CPS (16), ICS (14) and RAN & Mobile Devices (14), Power Systems (6), and Intelligent Transportation Systems (2). Across subdomains, AI & ML leads with 55 mentions, dominated by ICT (34) and complemented by CPS (9) and RAN & Mobile Devices (8). Dataset Generation is second with 36 mentions, driven by IoT, IIoT (15) and ICT (13), with additional use in Power Systems (3) and RAN & Mobile Devices (3), and single entries in CPS (1) and ICS (1). Data Science totals 13 and is mainly reported in ICT (8), ICS (3), and IoT, IIoT (2). Integrated Development Environment appears 11 times, led by ICT (5) and ICS (3), with smaller contributions in CPS (2) and IoT, IIoT (1). The remaining subdomains are sparse, with Backend Frameworks (8), Build-Toolchain (4), and Visualization & Dashboarding (4)

as the main secondary categories. Infrastructure, Middleware, Reverse Engineering and Binary Analysis, Runtime Environment, and Simulation Environment each occur only once. Overall, the heatmap shows that custom development is strongly data centric in ICT, with IoT, IIoT contributing substantial dataset generation work. CPS and RAN & Mobile Devices show notable AI and ML use but narrower breadth, while ICS activity is more concentrated in IDEs, visualization, and data science. Other domains exhibit isolated, domain specific instances.

AI & Machine Learning

An SDN-controlled IoT TB for DDoS attack detection uses TensorFlow as a machine-learning framework and Keras as a supporting library for AI and ML application development. The training datasets are captured separately from the raw traffic, and models are trained with different parameters whose results are compared and plotted to evaluate an efficient approach to DDoS detection at the core layer of the SDN-controlled TB [78]. In the SPIDER 5G CR, TensorFlow again acts as a machine-learning framework and Keras as a machine-learning library, both used as data-science tools to develop ML components that are then transferred into the CR. These ML tools support scenarios in a 5G-focused range that is built for complex cyber-attack scenarios and for the evaluation of cyber risk [145].

Dataset Generation

In one work on an SDN-based environment, commaseparated values (CSV) is used as the data format in which mean and standard deviation values obtained during data preprocessing are stored. This allows features to be normalized and made available for subsequent model training. In the same setting, the DPKT Python library is used for data processing and flow-feature calculation. The dataset providers supply code that computes the flow features using DPKT as part of the dataset-generation pipeline [142]. In a study that presents a comprehensive dataset of substation traffic for cybersecurity applications in substations, CSV is employed as the data format for network features, with two kinds of files added to the dataset: one containing traffic-related information and another containing a selected set of relevant features [65].

Data Science

In a work on dynamic and reliable intrusion detection, NumPy and Pandas belong to the Data Science subdomain and are used for feature extraction within the data-processing pipeline, supporting the intrusion-detection approach that aims to increase the system's robustness against motivated attackers [45]. In another study, NumPy and Pandas are used as part of the Python-based experimental setup for Data Science tasks, where they handle data management, support model training, and enable the implementation of graph algorithms, forming a core element of the data-science toolchain used to evaluate the proposed method against the considered attacks [141].

Integrated Development Environment

In an ICS-focused modular, open-source framework for assessing SCADA systems security, FUXA is used as an integrated development environment for HMI development, where the HMI component of the TB is implemented through the SCADA/HMI framework FUXA as part of the Target Infrastructure layer that supports the investigation of heterogeneous attack scenarios and security methodologies within the SCADA environment [44]. In an ICT cyber security TB that studies keyloggers, Jupyter notebook is used as an integrated development environment for keylogger development and data visualization, where the notebook is employed to write the code for the keylogger program and to support the visualization of keylogger-related data as part of demonstrating essential features of an effective cyber security TB [20]. In another ICT environment that introduces the TestCloudIDS dataset and the SparkShield IDS model, Jupyter notebook serves as the interface within an Anaconda-based setup, where PySpark and FindSpark packages are installed and the notebook acts as the integrated environment for configuring and running the SparkShield intrusion-detection model on the TestCloudIDS dataset [191].

Backend Frameworks

A CR exercise platform uses Flask as a backend framework to implement the REST API of a earning management system (LMS), where a VueJS-based LMS connects through this Flask API to the underlying Docker infrastructure as part of an incident-response CR exercise [60]. In a smart-grid Cyber Range as a Service, Flask provides the web application on the controller host that acts as the graphical user interface (GUI) for the range, which is described as a virtual environment on an OpenStack cloud platform [35]. For a privacy-preserving revocation mechanism based on a blockchain in the intelligent transportation systems domain, Node.js is used as the backend framework for a blockchain simulation environment that supports the proposed revocation mechanism and aims to reduce checking time and remove reliance on a single central authority [159]. In a Dockerized Android platform for mobile cyber-range scenarios, the backend module written in Node.js implements an extendible interface that controls actions such as dispatching a malicious SMS or e-mail to simulate phishing attacks within the mobile-focused cyber-range framework [30].

Visualization & Dashboarding

In an ICS TB for resilient operational systems, Ignition SCADA is used in the visualization and dashboarding subdomain to develop the SCADA UI, recreating industrial network environments and providing SCADA visualisation for OT protocols such as ModbusTCP and DNP3 within a virtual infrastructure that is coupled to a Typhoon-HIL real-time simulator [173]. In an ICS cyber-defense evaluation TB, Node-RED is employed in the visualization and dashboarding subdomain as the HMI environment, where a flow-based

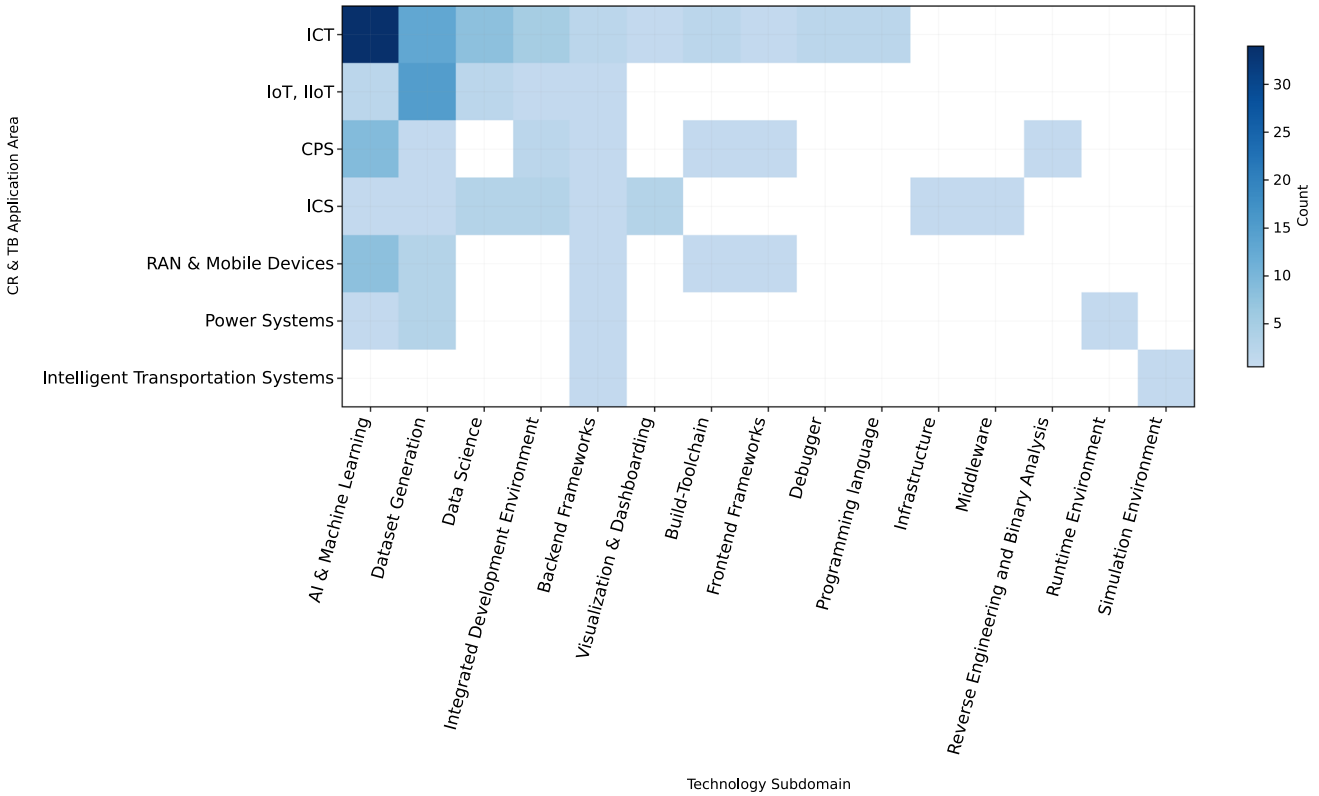


Fig. 12 Custom Development Subdomain Distribution Across Cyber Range Application Areas

programming approach is used to build the human–machine interface in a flexible hybrid/virtual TB that supports cyber-defense evaluation and comprehensive log collection from the TB [43].

Build-Toolchain

In the MaCySTe virtual TB for maritime cyber security, GNU Make is part of the build toolchain and is used to automate tasks in the TB, managing the execution of components and operations within the environment [99]. Within the NDIF framework for in-network neural-network–based applications in an ICT environment, the P4 compiler is used in the build toolchain to compile P4 programs that implement the in-network processing logic required by the framework [95].

Frontend Frameworks

In a work that introduces a CRX for incident response, VueJS is used for frontend development of the LMS, where the LMS communicates with the underlying Docker infrastructure via a REST API implemented with Flask, providing the web interface to the incident-response environment [60]. In a study proposing Dockerized cyber range components for mobile devices in next-generation cyber ranges, React.js is used to implement the UI, leveraging recent features together with TypeScript to create cohesive and loosely coupled frontend components for interacting with the range environment [30].

Debugger

In an ICT education environment that uses CTF-style exercises, Gdb and Gef are part of the debugger toolchain for the security exercise environment. Extensive tooling is provided so that students can work on challenges using these debuggers together with many other tools, in scenarios that cover CTF, CTFd, Linux usage, shell scripting, network security, web, kernel security, and microarchitecture speculative execution attacks within the same environment [120].

Programming language

In an ICT CR for cyber security exercises, Datalog is used as a programming language for formal scenario modelling. It provides a formal representation of exercise scenarios and supports verification of different scenario properties. This is implemented within a system that automates many cyber exercise tasks to support autonomy and skill improvement of participants in the range environment [206]. In an ICT CR that employs cyber attack and defense agents, Datalog is used as a programming language for formal modelling of agent decisions, specifying the agents' decision logic and enabling reasoning about decision properties such as whether the goal is fulfilled within the agent-based system that emulates cyber attacks and defenses in the range [207].

Infrastructure

In the SCASS modular, open-source framework for assessing SCADA systems security, Node-RED is deployed in the

SCADA-system container at the infrastructure layer. There, it realises SCADA process logic and HMI functionality. Within this ICS TB, Node-RED is used as a programming tool to model industrial processes and to support the design and execution of heterogeneous attack scenarios and security methodologies against the emulated SCADA environment [44].

Middleware

In an ICS cyber security education and gamification environment, OpenMUC is used as middleware at the Target Infrastructure layer to provide industrial process monitoring and control, enabling the monitoring and control of industrial components and processes within the TB [87].

Reverse Engineering and Binary Analysis

In a CPS security setting with mixed time and event-triggered moving target defense, Binary Ninja is used within the Reverse Engineering and Binary Analysis subdomain to translate binaries to LLVM bitcode, providing binary disassembly and control-flow recovery as part of the analysis pipeline [131].

Runtime Environment

In a power-systems CR that imitates a smart grid configuration on an OpenStack cloud platform, Open Java Development Kit (OpenJDK) 8 is used as the runtime environment inside a controller container, providing the Java-based tools required to run controller functionality and to support automated cybersecurity experiments and training within the virtual environment [35].

Simulation Environment

In an intelligent transportation systems environment that proposes a privacy-preserving revocation mechanism for vehicular ad hoc networks (VANETs) with a blockchain using accumulators, cpprestsdk is used in the Simulation Environment at the Target Infrastructure layer as a REST API library to integrate the VANETs infrastructure with Hyperledger Composer's REST API, enabling communication between the VANETs infrastructure and the blockchain-based revocation components within the TB [159] (Table 5).

4.3.6 Blue team operations

This *technology domain* covers blue team technologies used across CRs and TBs. Figure 13 quantifies coverage by *application area* and subdomain. ICT shows the highest overall activity with 46 mentions, followed by ICS (30), RAN & Mobile Devices (11), Power Systems (9), CPS (6), IoT/IIoT (6), and Intelligent Transportation Systems (1). Across subdomains, Intrusion Detection & Prevention (IDS/IPS) leads with 27 mentions. security information and event management (SIEM) & Security Analytics and Vulnerability Management follow with 23 mentions each. Network Analysis & Reconnaissance totals 11, while the remaining subdomains show lower coverage, including Firewalls & Network Security Gateways (5), Training and Practice Systems (4), Malware Analysis (3), and Threat Intelligence (3). Endpoint Detection & Response (endpoint detection and response (EDR)), Phishing and Social Engineering, and Reverse Engineering and Binary Analysis appear 2 times each, while Application Security Testing, Deception & Honeypot Systems, Incident Management & Response, and Security Hardening each occur once. At the *application area* level, IDS/IPS is strongest in ICS (10) and ICT (9), with additional use in Power Systems (7) and IoT/IIoT (1). SIEM & Security Analytics is concentrated in ICT (13) and ICS (6), with further activity in IoT/IIoT (3) and CPS (1). Vulnerability Management is broadly represented and is driven by ICT (8), RAN & Mobile Devices (7), and CPS (5), with single entries in ICS, IoT/IIoT, and Intelligent Transportation Systems (1 each). Network Analysis & Reconnaissance is strongly concentrated in ICS (8) and appears only marginally in ICT, IoT/IIoT, and RAN & Mobile Devices (1 each). Overall, the heatmap indicates a defensive stack that is centreed on detection and telemetry, where IDS/IPS and SIEM dominate as the primary components. This stack is supplemented by vulnerability management and targeted analyses, with ICT and ICS providing the widest and deepest coverage.

Intrusion Detection & Prevention (IDS/IPS)

In an ICS emulation environment (RESlab), Snort is configured to detect scanning attempts, where for each Nmap port scan experiment the scripts start Snort to identify suspicious ports and attack patterns as part of evaluating the reproducibility of adversary network scanning detection within the lab [178]. Another ICS TB deploys Snort v3.0 with snort3 community rules as a signature-based network intrusion detection system (NIDS) that detects known attack patterns, forming the central intrusion-detection component in a dynamic and reliable IDS approach designed to increase robustness against motivated attackers within the industrial control environment [45]. In an ICS TB that aims to create a controlled and reproducible environment for a WWTP industrial process, Suricata is used as the primary tool for network threat detection, analysing traffic in order to distinguish malicious activity from normal activity and thus support security assessment of the industrial process [101]. In an ICT setting that introduces a graph-based analysis of cyber attacks, Suricata communication alerts are combined with ATT&CK alerts and other log events to construct evidence paths and build a kill chain attack graph, so that the Suricata alerts become key elements in correlating detected events and assessing attack severity within the TB [152].

SIEM & Security Analytics

In an ICS TB that aims to create a controlled and reproducible virtual environment for a WWTP industrial process, Security Onion is deployed for network and system monitoring and is used as a security information and event manage-

Table 5 Top-10 Technologies per Subdomain for Custom Development. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
AI & Machine Learning	55	29	TensorFlow† (12), Keras† (4), Scikit-learn† (4), PyTorch† (3), Transformers† (3), Anaconda† (2), Google Colab† (2), NumPy† (2), Pandas† (2), Seaborn† (2)	CPS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Backend Frameworks	8	6	Flask*† (2), Node.js† (2), Java Spring† (1), Python Flask framework† (1), Spring Boot† (1), pyModbus† (1)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Build-Toolchain	4	4	GNU Make* (1), P4 Compiler† (1), Setuptools† (1), asn1c tool† (1)	CPS, ICT, RAN & Mobile Devices
Data Science	13	5	NumPy† (5), Pandas† (5), DESLib (Dynamic Ensemble Selection Library)† (1), Keras† (1), Scipy† (1)	ICS, ICT, IoT, IIoT
Dataset Generation	18	9	CSV† (10), Apache Parquet† (1), DPKT† (1), HERA† (1), IPAL Toolset† (1), MySQL Workbench† (1), PCAPNG† (1), Pandas† (1), Zeek† (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Debugger	2	2	Gdb† (1), Gef† (1)	ICT
Frontend Frameworks	3	2	React.js† (2), VueJS* (1)	CPS, ICT, RAN & Mobile Devices
Infrastructure	1	1	Node-RED† (1)	ICS
Integrated Development Environment	11	7	Jupyter notebook† (3), FUXA† (2), Node-RED† (2), ABB Automation Builder IDE† (1), Arduino IDE† (1), Ipython† (1), Step7-MicroWin† (1)	CPS, ICS, ICT, IoT, IIoT
Middleware	1	1	OpenMUC† (1)	ICS
Programming language	2	1	Datalog† (2)	ICT
Reverse Engineering and Binary Analysis	1	1	Binary Ninja† (1)	CPS
Runtime Environment	1	1	OpenJDK 8† (1)	Power Systems
Simulation Environment	1	1	cpprestsdk† (1)	Intelligent Transportation Systems
Visualization & Dashboarding	4	4	Ignition SCADA† (1), Node-RED† (1), OPC Unified Architecture (OPC-UA)† (1), PrettyTable† (1)	ICS, ICT

ment platform within the multi-layered architecture [101]. In a smart airport cybertwins security TB for IIoT environments, Security Onion provides network security monitoring, data collection, and intrusion detection, where a tap machine records network traffic and the collected data is managed through a dedicated data management tool as part of evaluating attack and defence scenarios [84]. Within a crisis management exercise that trains cyber security professionals in decision-making, Wazuh SIEM is installed to monitor networks and endpoints, and its interface is used to confirm that traffic was generated and observed during the exercise as part of the scenario-based evaluation [149]. In a TB that introduces CyberAlly, a knowledge graph-enhanced AI assistant for cyber defence, Wazuh SIEM provides alert monitoring, where participants observe Wazuh posting alerts that are then correlated, filtered, and analysed by CyberAlly to support the investigation of incidents and the recommendation of defensive actions [81].

Vulnerability Management

In a study that introduces next-generation tools for developing cyber-security applications, Nessus is used for remote vulnerability scanning. Nikto is included as part of the defen-

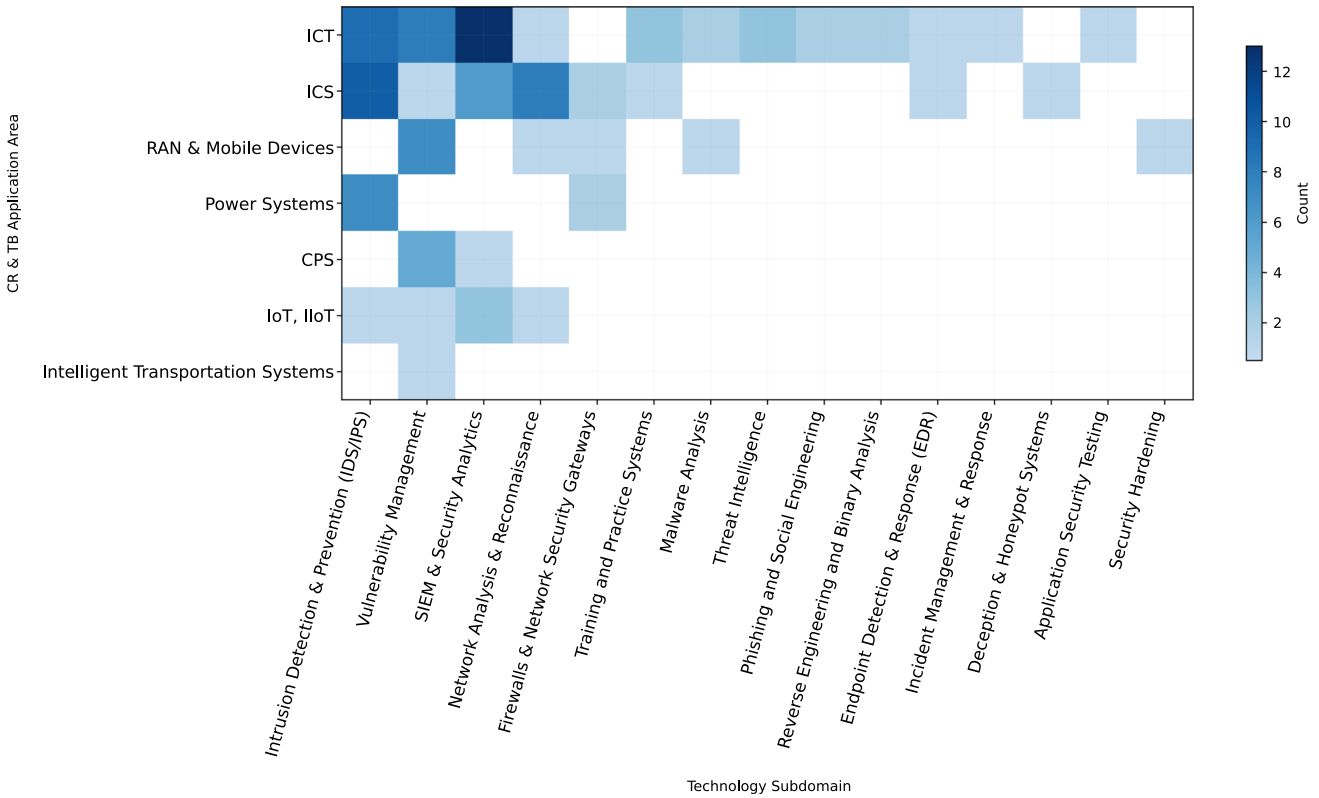


Fig. 13 Blue Team Operations Subdomain Distribution Across Cyber Range Application Areas

sive tool set. Each application in this environment provides either attack (red-teaming) or defense (blue-teaming) mechanisms to support the assessment of security readiness against real-life cyber-attacks within the CR [3]. A CR TB environment for evaluating security orchestration, automation, and response (SOAR) tools relies on Nessus for vulnerability scanning of the entire network, where periodic scans (with their associated logs recorded at fixed intervals) are used to characterise the security posture of the environment and to provide input to the analysis of SOAR behaviour [27]. In an experimental setup that examines the security of web-based communications in solar DG systems, Nikto is applied to assess the security of the web interfaces, alongside other web-security tools, as one step in a broader evaluation of security controls intended to enhance the overall cybersecurity posture of the system [115].

Network Analysis & Reconnaissance

A remote cyber security training platform built around control cabinets with automation and control equipment uses Nmap for system discovery tasks, giving students practical experience with discovering and recognizing systems in the training environment, while Wireshark is employed in hands-on exercises to capture and analyse network traffic generated by the control system in operation within the same remote training setup [49]. In a reservoir TB used for cyber security exercises, Wireshark is employed by the attacker to determine the used network segment, providing visibility into the network configuration of the target environment as a preparatory step for subsequent actions against the devices such as PLCs and HMIs deployed in the TB [176].

Firewalls & Network Security Gateways

Iptables/nftables are deployed in an ICS TB as firewall rules on top of an Ubuntu 22.04 operating system, where they regulate OT network traffic and are configured based on related work to support the evaluation of a dynamic and reliable intrusion-detection method against motivated attackers within the emulated SCADA environment [45]. In a framework for the security evaluation of RAN and mobile-device environments connected to non- and near-real-time Radio Intelligent Controllers (RIC), IPsec / IKEv2 is configured at the operating-system level to establish two IPsec tunnels, ensuring the confidentiality and integrity of communication between the evaluated environment, the RIC, and the O-CU [86].

Training and Practice Systems

One training and practice setup is built around a cyber-range platform that uses open-source tools to create an isolated network infrastructure with VPN access and supporting tools. In this environment, WordPress is included as part of a forensic analysis and practice setting. Trainees can flood a target IP, trigger record alerts, and generate log files so that they can work through incident-focused exercises on a dedicated

training network[192]. A second example uses the EVE-NG platform as the basis for a cyber-range environment in which Fortinet's web application firewall, Fortinet's logging components, and Huawei's firewall are deployed as trial devices inside a simulated network. The overall setup provides an infrastructure environment for network attack and defence exercises that allows learners to practise configuring and evaluating these security controls in realistic training scenarios[138].

Malware Analysis

A CR TB environment configured for testing SOAR tools integrates ThreatGrid in the cloud alongside a Jira instance for ticketing and a dedicated email system, using ThreatGrid for malware sandbox testing as part of the analysis of artifacts delivered through this setup [27]. Within a security TB for next-generation systems, URLhaus is used in a simple malware-analysis case to validate that collected URLs are malicious and are being used for malware distribution, allowing the TB to measure or compare how well a given defense mechanism performs against such malicious URLs [112].

Reverse Engineering & Binary Analysis

In the DOJO applied cybersecurity education environment, Ghidra and Radare2 are used as reverse engineering and binary analysis tools within a security exercise setting, where extensive tooling is provided and students work on challenges in a unified environment. These tools are available in CTF and CTFd-based activities that cover Linux usage, shell scripting, network security, web-related topics, kernel security, and microarchitecture speculative execution attacks within the same training setup [120].

Phishing Detection & Anti-Spoofing Tools

A case study on mitigating injection and phishing attacks in an ICT environment uses PhishDetector and PhishTor for web page classification, so that phishing-related pages can be identified and filtered as part of a setup that addresses security attacks associated with plugins and aims to proactively implement a secure environment [23].

Threat Intelligence

In an ICT cyber defence environment that introduces CyberAlly, a knowledge graph–enhanced AI assistant for SOC operations, MITRE ATT&CK is used as an information source for GPT, supplying structured threat knowledge that the assistant leverages to support analysts with context-aware recommendations based on previous red-versus-blue exercises [81]. A second ICT scenario presents a graph-based approach for incident triage, where MITRE ATT&CK is integrated into a severity-based triage method that combines custom kill-chain–based attack graphs with asset criticality, so that MITRE ATT&CK tactics and techniques become part of the reasoning used to prioritise cybersecurity incidents [152].

Endpoint Detection & Response (EDR)

A cyber range test environment for evaluating SOAR tools integrates Endgame as the endpoint detection and response component within a full SOC tool suite, alongside Elasticsearch and Kibana as SIEM and Suricata as NIDS, enabling endpoint-focused monitoring and investigation across multiple representative threat-emulation scenarios [27]. The hybrid SDN-based ICS security proof-of-concept uses pigrelay as an alert-forwarding component: Snort runs in network socket mode and a pigrelay script relays its alerts to the SDN controller, supporting detection and response to network-channel attacks in the evaluated industrial environments [102].

Incident Management & Response

Within the DefAtt virtual cyber-labs platform for network-security education and training, anomalies detected in the monitored environment trigger alerts that are forwarded to TheHive, which is used for incident management by collecting and processing these alerts as part of handling network-based attacks and their defences in the highly automated range. [104].

Deception & Honeypot Systems

An ICS TB for evaluating a dynamic and reliable intrusion-detection approach deploys Honeyd v.1.5c as a honeypot, mirroring incoming network traffic to another ScadaBR server and thereby supporting the assessment of the proposed method against motivated attackers within the SCADA environment [45].

Application Security Testing

In an ICT virtual environment that automates security scenarios and their deployment using Ansible, Contrast Security is used in the Application Security Testing subdomain as a blue-team mechanism, acting as a defensive application within a set of apps that each provide either attack (red-teaming) or defense (blue-teaming) capabilities to assess security readiness against real-life cyber-attacks within the range environment [3].

Security Hardening

In a framework for the security evaluation of O-RAN mobile network equipment connected to non- and near-real-time RIC, a virtual machine running Ubuntu is secured by applying a hardening procedure based on the Ubuntu Security Guide for centre for Internet Security (CIS)-compliant Ubuntu long-term support (LTS), so that the CIS Ubuntu Security Guide provides the concrete baselsine for hardening the evaluated environment [86] (Table 6).

4.3.7 Portal services

This *technology domain* covers portal services used across CRs and TBs. Figure 14 quantifies coverage by domain and subdomain. ICT exhibits the highest overall activity with 19 mentions, followed by RAN & Mobile Devices (6), ICS (5), Power Systems (3), and IoT/IIoT (1). AAcross subdomains,

Table 6 Top-10 Technologies per Subdomain for Blue Team Operations. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Application Security Testing	1	1	Contrast Security† (1)	ICT
Deception & Honeypot Systems	1	1	Honeyd† (1)	ICS
Endpoint Detection & Response (EDR)	2	2	Endgame† (1), pigrelay† (1)	ICS, ICT
Firewalls & Network Security Gateways	5	5	IPsec / IKEv2† (1), Iptables/nftables† (1), PfSense† (1), Suricata† (1), untangle† (1)	ICS, Power Systems, RAN & Mobile Devices
Incident Management & Response	1	1	TheHive† (1)	ICT
Intrusion Detection & Prevention (IDS/IPS)	27	7	Snort† (11), Suricata† (8), Zeek† (3), OSSEC† (2), Security Onion† (1), Wazuh HIDS† (1), scapy† (1)	ICS, ICT, IoT, IIoT, Power Systems
Malware Analysis	3	3	ThreatGrid† (1), URLhaus† (1), VirusTotal† (1)	ICT, RAN & Mobile Devices
Network Analysis & Reconnaissance	11	5	Wireshark† (6), Tshark† (2), Nmap† (1), Shodan† (1), Zeek† (1)	ICS, ICT, IoT, IIoT, RAN & Mobile Devices
Phishing and Social Engineering	2	2	PhishDetector† (1), PhishTor† (1)	ICT
Reverse Engineering and Binary Analysis	2	2	Ghidra† (1), Radare2† (1)	ICT
SIEM & Security Analytics	23	14	Security Onion† (4), Wazuh SIEM† (4), ELK Stack† (2), Elasticsearch† (2), Kibana† (2), Dsiem† (1), Elastic Security (SIEM)† (1), GPT-4o† (1), JSON‡ (1), MobSF (Mobile Security Framework)† (1)	CPS, ICS, ICT, IoT, IIoT
Security Hardening	1	1	CIS Ubuntu Security Guide† (1)	RAN & Mobile Devices
Threat Intelligence	3	1	MITRE ATT&CK† (3)	ICT
Training and Practice Systems	4	4	Fortinet's WAF (15-day trial):† (1), Fortinet's log (15-day trial):† (1), Huawei's firewall (30-day trial)† (1), Wordpress† (1)	ICS, ICT
Vulnerability Management	23	19	Nessus† (2), Nikto† (2), OpenVAS† (2), Owasp Zap (Zed Attack Proxy)† (2), CVSS† (1), Clang-tidy† (1), InsightVM† (1), MITRE CAPEC† (1), MITRE CWE† (1), NIST Randomness Test Suite† (1)	CPS, ICS, ICT, IoT, IIoT, RAN & Mobile Devices

User Access dominates with 25 mentions. Admin Access (4) and Authentication (2) are less frequent. Identity & Access Management (identity and access management (IAM)) (2) and Authorization (1) are rare. By domain–subdomain detail, User Access is concentrated in ICT (13) with further use in RAN & Mobile Devices (5), ICS (4), Power Systems (2), and IoT/IIoT (1). Admin Access appears in ICT (3) and Power Systems (1). Authentication is reported only in ICT (2). IAM is recorded in ICS (1) and RAN & Mobile Devices (1). Authorization occurs once in ICT (1). Overall, portal services in the dataset focus primarily on user access, with administrative, authentication, and identity-centric controls documented selectively and largely centreed in ICT, while ICS contributes isolated IAM usage and RAN & Mobile Devices adds targeted access-management entries.

User Access

In an Industry 4.0–focused cyber-range platform, OpenSSH is used to provide shell access and file transfers (via secure copy protocol (SCP)) to the containerised training environment, enabling administrators and instructors to configure Docker containers on the server and manage the open-source services that underpin the cyber range [192]. Within the DOJO applied cybersecurity education environment, OpenSSH underpins student environment access by allowing

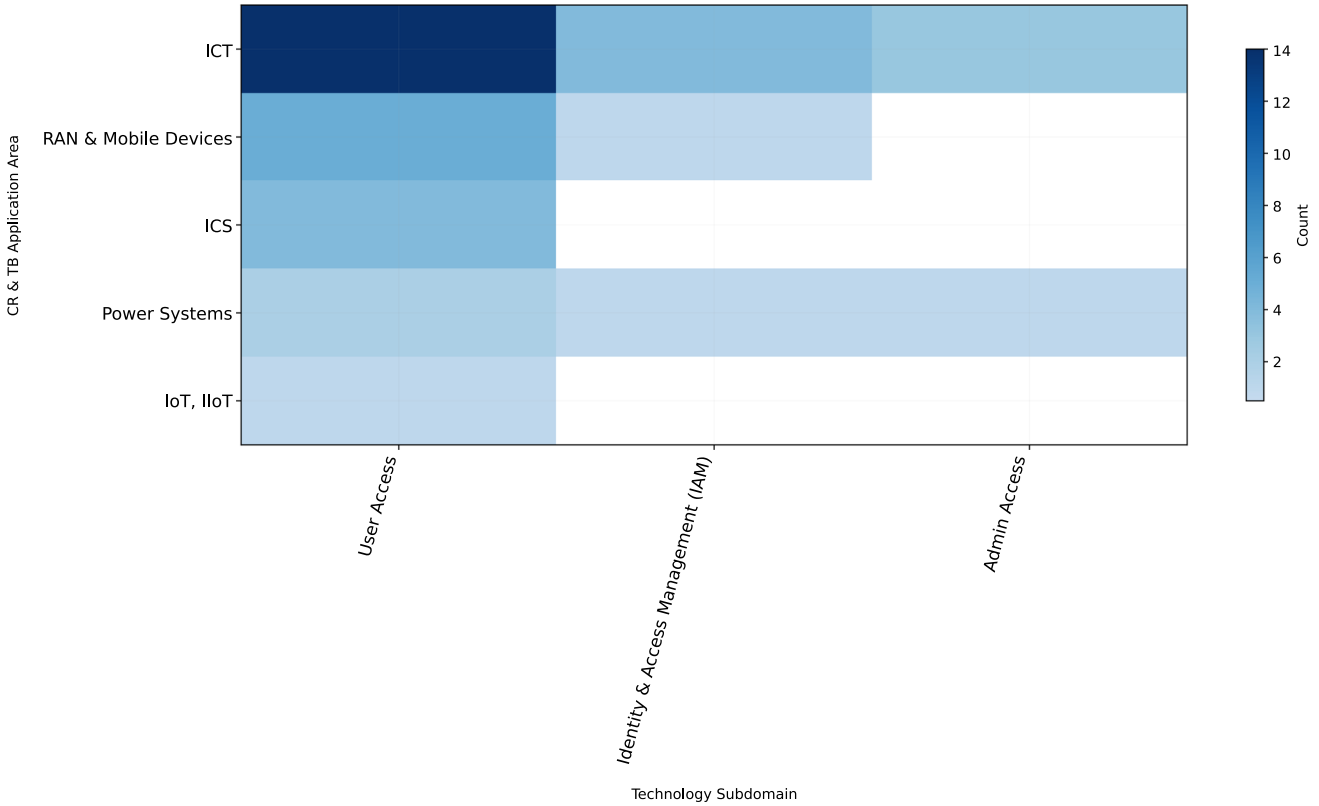


Fig. 14 Portal Services Subdomain Distribution Across Cyber Range Application Areas

learners to upload a public key and then log in to their individual Linux-based training instances, supporting CTF-style exercises and hands-on practice in shell scripting, networking, and related topics [120]. In the Cyber Arena platform for scalable cybersecurity education, Apache Guacamole provides browser-based remote access for students, with a Guacamole server exposed via a public IP so that learners can reach their lab environments from any Internet location through a web interface without installing additional client software [68]. In an IoT/IIoT security training environment for system developers, Apache Guacamole is employed for Linux container access management, where user access to containerised training instances is handled through the Guacamole gateway as part of a methodology that integrates IoT security topics into project-based learning [18].

Admin Access

In a crisis-management exercise environment where organisations undergo simulated cyberattacks, OpenSSH is installed and enabled on all machines to provide secure shell (SSH) connections, so that administrators can remotely access and manage the hosts over SSH as part of training cyber security professionals in decision-making within the exercise setup [149]. In a power-systems infrastructure for electrical substations used for testing and evaluation of cyber-attacks and incident response procedures, Apache Guacamole offers browser-based remote access into the enclave environment, enabling administrators to reach systems inside the substation TB through a secure web interface during cyber-attack evaluation and training activities [69].

Identity & Access Management (IAM)

In a cyber-range technology platform that combines virtual and hands-on components to enable higher levels of experiential learning, Authentik is deployed as the central identity and access management system for the Proxmox-based infrastructure, while DUO two-factor authentication (2FA) adds multi-factor authentication (MFA) by providing a plugin-backed mechanism to store and generate one-time passcodes (OTPs) for user logins. [66] In an ICT environment used to evaluate a new graph-based approach for incident handling, Windows Active Directory provides authentication and role management for all workstations and servers in the internal Windows domain, with the domain infrastructure (including the Active Directory and DNS servers) supplying the host context whose alerts are later analysed by the proposed triage method. [152] A power-systems security study uses Windows Active Directory within the centre Energy TB architecture, where OSSEC agents run on machines at multiple levels and some field-device controllers use Windows-based operating systems, so that domain-based authentication and role

Table 7 Top-10 Technologies per Subdomain for Portal Services. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Admin Access	4	2	Apache Guacamole*† (2), OpenSSH† (2)	ICT, Power Systems
Identity & Access Management (IAM)	6	4	Windows Active Directory† (2), Authentik† (1), DUO 2FA* (1), OAuth 2.0† (1)	ICT, Power Systems, RAN & Mobile Devices
User Access	26	12	OpenSSH*† (7), Apache Guacamole*† (3), Virtual network computing (VNC)† (3), Windows Remote desktop protocol (RDP)† (3), NETLAB+† (2), JupyterHub‡ (1), Tmux† (1), VS Code† (1), Wireguard* (1), srcpy† (1)	ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices

management support the defence-in-depth structure of the evaluated energy-system test environment. [127] (Table 7)

4.3.8 Management

This *technology domain* covers management functions used across CRs and TBs. Figure 15 quantifies coverage by *application area* and subdomain. ICT leads overall with 18 mentions, followed by ICS (7). IoT/IIoT and Power Systems each account for 2 mentions, and Intelligent Transportation Systems accounts for 1. Across subdomains, Platform & Environment Management is most common (7), followed by Identity & Access Management (IAM) (5). Asset & Infrastructure Management and Learning Management System each total 4. Operations Management and User Management each total 3. Content and Document Management and Workflow & Orchestration each total 2. ICT provides the broadest functional spread and covers all listed management subdomains, with the highest values in Learning Management System (4), Operations Management (3), and User Management (3). ICS is strongly concentrated in Platform & Environment Management (5) and contributes Identity & Access Management (2). Power Systems reports only Asset & Infrastructure Management (2). IoT/IIoT reports Platform & Environment Management (1) and Workflow & Orchestration (1). Intelligent Transportation Systems reports a single entry in Identity & Access Management (1). Overall, management capabilities are anchored in ICT, while other *application areas* show narrow coverage that is mainly platform administration in ICS and asset management in Power Systems.

Platform & Environment Management

The DOJO applied cybersecurity education platform relies on 9p for transparent file-system mapping between QEMU virtual machines and containers, so that the learner's environment can access files seamlessly across VMs and container boundaries in CTF-style browser-based labs covering topics from Linux usage to microarchitecture attacks [120]. In the CyberIoT web-based cyber range for IoT, a Linux, Apache, MySQL, and PHP (LAMP) stack hosts the three-tier web application, where LAMP provides the web and database tiers that support instantiation, execution, and operation of IoT-focused cybersecurity training exercises [162].

Identity & Directory Access Management (IAM)

Windows Active Directory is used in a large-scale ICT cyber range architecture to provide virtualised directory and authentication services, where Active Directory, DNS, and domain controller roles are deployed to manage users and systems consistently across the range environment [126]. The ecurity Credential Management System (SCMS) appears in an intelligent transportation systems co-simulation platform for connected and automated driving, where it enables secure and privacy-aware communication between devices by handling certificate-based credentials for exchanging information in the test environment [1].

Learning Management System

The Tectonic academic cyber range uses Moodle to deliver and collect assessments, where students submit flags and complete questionnaires via the Moodle platform so that evaluation of their performance is tightly coupled to the range's training scenarios [64]. In the ETHACA container-based cyber range, Moodle is deployed as an open-source learning management system to improve educational outcomes and monitoring, with the LMS integrated into the open-source cyber range infrastructure alongside other components for strengthening cybersecurity learning experiences [37]. The CyberSim Lab environment integrates the Bazaar Collaborative Learning Environment as a collaborative learning platform that supports cybersecurity labs, where Bazaar underpins activities designed around specific learning outcomes and fosters collaborative learning, technical simulation, and metacognitive engagement across different learner groups [124].

Asset & Infrastructure Management

Within the CENTER Energy secure TB for electricity power grids, Dragos OT Asset Visibility and Inventory is used to provide asset visibility and maintain an inventory of OT components, while Windows Active Directory handles

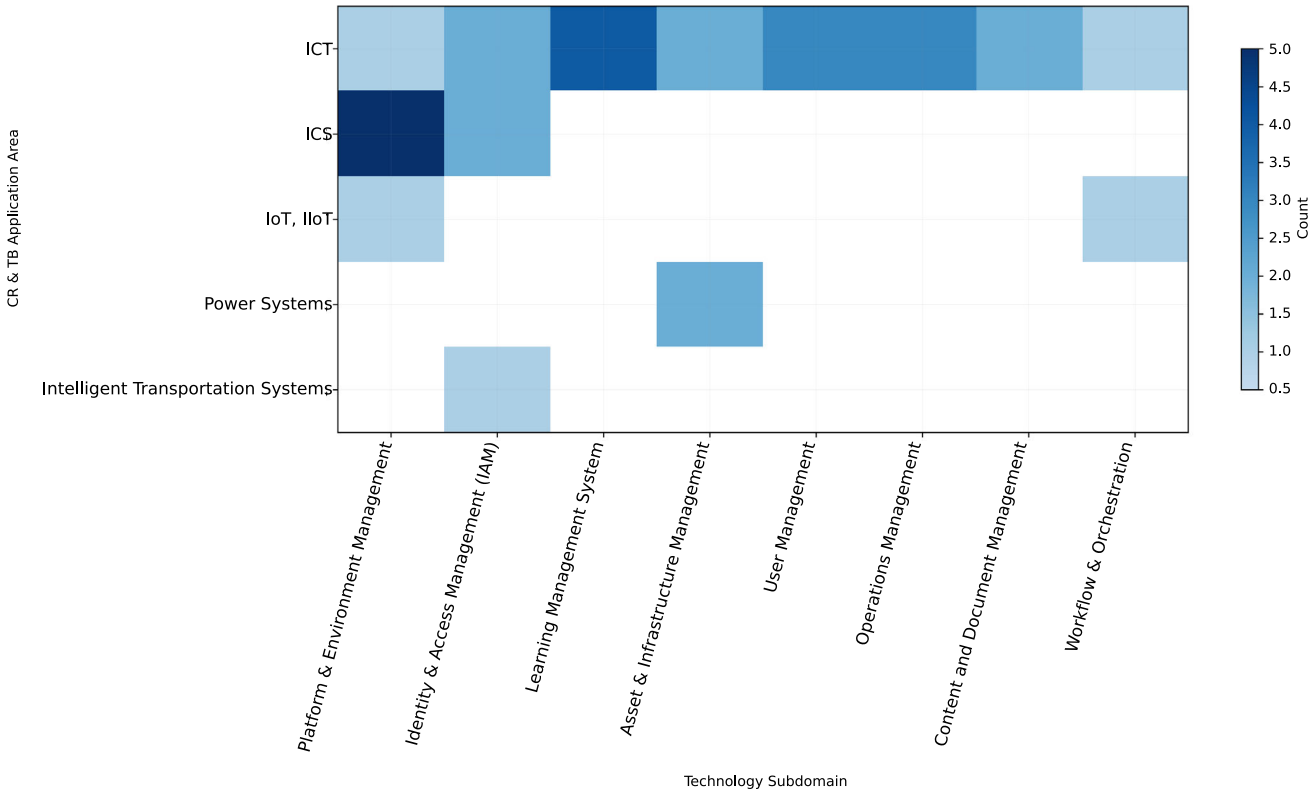


Fig. 15 Management Subdomain Distribution Across Cyber Range Application Areas

authentication and role management for all Windows-based workstations and servers in the environment [127]. The KYPO-CRP-based smart-grid cyber range uses GIT as the versioning backend for scenario, device, and network descriptions, storing these elements as text files that are uploaded and maintained in the platform via the GIT repository [94].

User Management

The CyberExpert platform for cybersecurity expertise acquisition uses CSV as a structured data-exchange format for student information, with scripts that read CSV files to automate new-user creation and populate accounts in the mixed virtual and hands-on cyber-range environment [66]. In a cyber-range exercise design environment, user data management is implemented with Google Firebase, which stores and manages participant information needed by the exercise portal and related components in line with the interdisciplinary CRX design principles [60].

Operations Management

A SOAR-focused cyber range TB environment configures Jira as the ticketing and incident-management system in the cloud, using Jira to manage tickets generated during security-orchestration experiments and to support the overall workflow around testing SOAR tools [27]. For log-based anomaly detection on cyber range platforms, Pm4py is employed to perform process-mining analysis on collected logs, providing process discovery and conformance checking that help analyse attack scenarios such as path traversal with remote code execution and privilege escalation [24].

Content and Document Management

A large-scale ICT cyber range architecture employs SharePoint as a collaboration and documentation platform for distributing training materials and exercise artefacts, and the same environment runs Windows Active Directory to provide virtualised Active Directory, DNS, and domain controller services for managing users and systems across the range [126]. Wordpress serves as the content management system in a cloud-based cyber range blueprint for low-cost security research, where it is used for the "Imitating Human Behaviour" component that structures and delivers web content required by the range design [195].

Workflow & Orchestration

The CyberAlly environment integrates Cydarm as a case-management backend for workflow and orchestration, where CyberAlly generates and links task tickets in Cydarm so that suspicious alerts can be handled efficiently within the incident-response process [81]. Within the SAir-IIoT cyber TB for smart airports, JSON serves as the data format for configuration and labelling of network-traffic analysis data, supporting the definition and handling of attack and

Table 8 Top-10 Technologies per Subdomain for Management. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Asset & Infrastructure Management	3	3	Dragos OT Asset Visibility and Inventory† (1), GIT† (1), YAML‡ (1)	ICT, Power Systems
Content and Document Management	2	2	SharePoint† (1), Wordpress† (1)	ICT
Identity & Access Management (IAM)	5	2	Windows Active Directory† (4), Security Credential Management System (SCMS)* (1)	ICS, ICT, Intelligent Transportation Systems
Learning Management System	4	2	Moodle† (3), Bazaar Collaborative Learning Environment† (1)	ICT
Operations Management	3	3	Jira† (1), Pm4py† (1), ProM† (1)	ICT
Platform & Environment Management	7	7	9p† (1), LAMP stack† (1), OpenPLC† (1), PARCS† (1), R5† (1), WinSCP† (1), scapy† (1)	ICS, ICT, IoT, IIoT
User Management	3	3	CSV† (1), Google Firebase* (1), OpenLDAP† (1)	ICT
Workflow & Orchestration	2	2	Cydarm† (1), JSON† (1)	ICT, IoT, IIoT

defence scenarios in IIoT-based smart-airport experiments [84] (Table 8).

4.3.9 Network infrastructure

This *technology domain* describes technologies used exclusively in the Core Technology layer and covers network infrastructure capabilities that support CRs and TBs. Figure 16 quantifies coverage by *application area* and subdomain. ICT leads with 19 mentions, followed by ICS (13), Power Systems (11), IoT/IIoT (9), CPS (4), and RAN & Mobile Devices (1). Across subdomains, Network Virtualization dominates with 46 mentions, Firewall and routing platform accounts for 10, and Reverse Proxy appears once. Network Virtualization is reported in all *application areas* and is most frequent in ICT (14), Power Systems (10), and ICS (9), with additional mentions in IoT/IIoT (8), CPS (4), and RAN & Mobile Devices (1). Firewall and routing platform is concentrated in ICT (4) and ICS (4) with single entries in IoT/IIoT (1) and Power Systems (1). Reverse Proxy is observed only once in ICT. Overall, the data show that virtualized networking forms the backbone of connectivity across *application areas*, while firewall and routing platforms provide selective perimeter functions and reverse proxy usage is rare.

Network Virtualization

An autonomous-operations TB for OT plants places the entire OT network into a single Mininet instance, allowing diverse attack types that lead to plant instability to be initiated and observed within a controlled virtual network [140]. An ICS-focused cyber range for evaluating authentic training exercises uses Mininet as the network simulation tool to emulate industrial control-system communication within the range, so that the framework can instantiate and assess exercises such as Iceberg CRX under realistic virtual network conditions [61]. An SDN-based ICS proof of concept for detection and response employs OpenvSwitch (OvS) as the OpenFlow switch that realises the network simulation between Snort and the RYU SDN controller when assessing industrial environments that are not time sensitive [102]. The DefAtt automated framework for network-based attacks and defences uses an OvS engine to construct the underlying infrastructure, creating bridges and ports to which virtual machines and Docker containers are attached for security evaluation [104].

Firewall and routing platform

One multi-faceted cybersecurity TB, TROY, deploys eight pfSense 2.6 firewalls to build subnets and DMZs, with each firewall filtering and forwarding traffic between segments to support comparison of open-source cybersecurity datasets and TBs [158]. A different virtualised environment places a pfSense-based VM at the centre of the TB, where it combines firewall and routing functionality to segment traffic between the management server, cluster servers, and the Internet while Modbus protocol vulnerabilities are explored [196]. A cyber-defence exercise setup for university students applies OPNSense to enforce policies between multiple subnets and to provide routing and firewalling, with the same

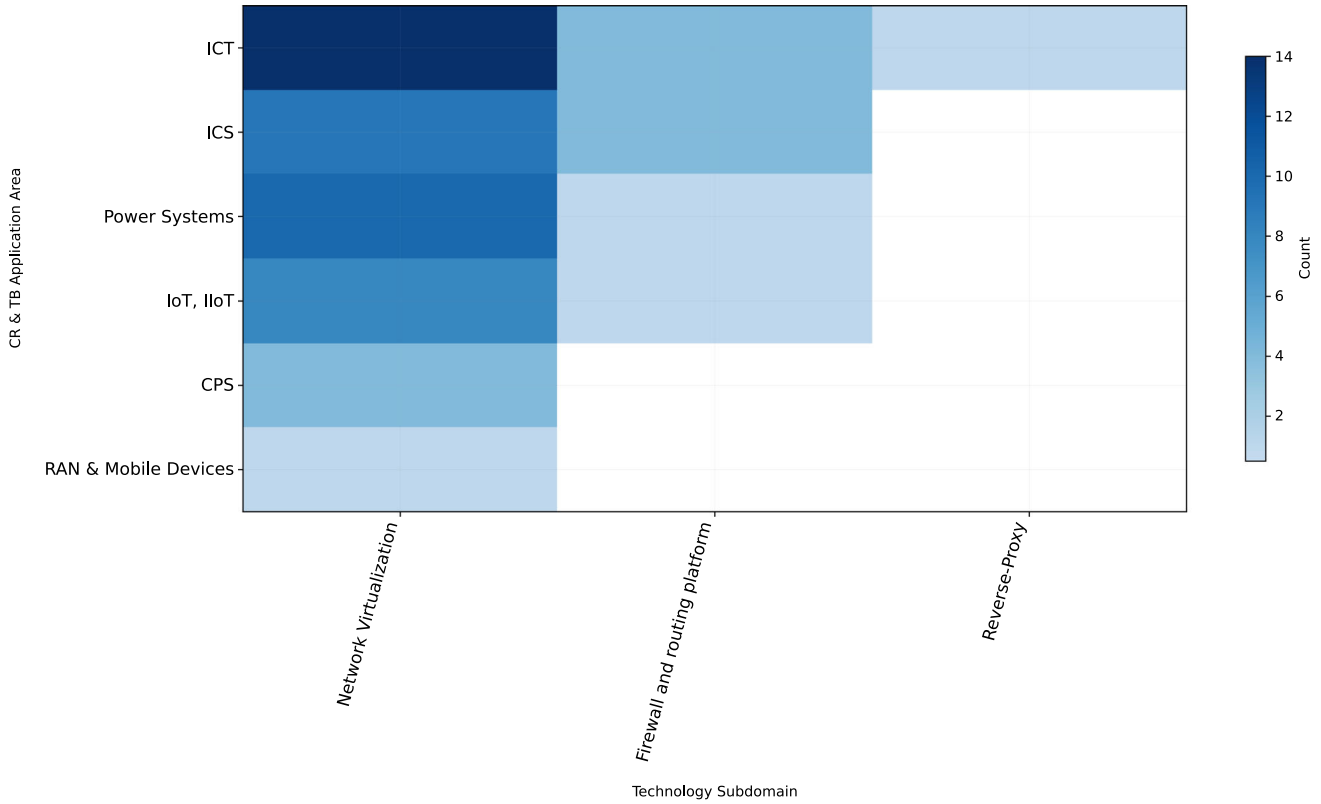


Fig. 16 Network Infrastructure Subdomain Distribution Across Cyber Range Application Areas

instance linking the enterprise part of the environment to a simulated Internet for realistic traffic conditions [151]. Log-analysis–oriented anomaly-detection experiments rely on an OPNSense VM running on a Proxmox server as the firewalling component that protects the infrastructure whose logs are analysed for path traversal, remote code execution, and privilege-escalation scenarios [24].

Reverse-Proxy The CyberExpert technology platform, which combines virtual and hands-on components, front-ends its cyber-range services with Nginx Proxy Manager to provide a secure and easy-to-manage reverse proxy and load-balancing layer that supports higher levels of experiential learning [66] (Table 9).

4.3.10 Scenario

This domain describes the technologies used to implement a wide range of scenarios in CRs and TBs. Figure 17 quantifies coverage by *application area* and scenario subdomain. Overall activity is highest in ICT and Power Systems with 107 mentions each, followed by ICS (106), CPS (92), RAN & Mobile Devices (66), IoT/IIoT (51), and Intelligent Transportation Systems (39). Across subdomains, Infrastructure dominates with 316 mentions, followed by Simulation and Emulation (125), Create/Edit (66), and Traffic Generation (46). Controlling is reported 13 times. User Activity Simulation and User behaviour Simulation appear once each and only in ICT. At the *application area* level, ICS and Power Systems primarily emphasise Infrastructure (63 and 61) and Simulation and Emulation (27 and 26). ICT combines Infrastructure (55) with Create/Edit (27) and Traffic Generation (20), while the remaining subdomains occur only marginally in ICT. CPS shows a near balance between Infrastructure (43) and Simulation and Emulation (39). RAN & Mobile Devices remains infrastructure focused (47) with smaller counts in the other subdomains. IoT/IIoT pairs Infrastructure (32) with notable Traffic Generation (16). Intelligent Transportation Systems is distinct because Simulation and Emulation (22) exceeds Infrastructure (15). Overall, scenario implementations remain infrastructure centric across most *application areas*, with simulation and emulation as the main complementary activity. Create/Edit and traffic generation are concentrated in ICT and IoT/IIoT, while user behaviour oriented simulation is almost absent in the analysed literature.

Infrastructure

A smart-grid TB uses two Ubuntu virtual machines running rapid-SCADA and pySCADA to retrieve power-system statistics from PLCs via the Modbus TCP protocol, store these data in an SQL database, and expose them through

Table 9 Top-10 Technologies per Subdomain for Network Infrastructure. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Firewall and routing platform	10	4	PfSense*† (5), OPNSense* (3), IPFire * (1), Iptables/nftables* (1)	ICS, ICT, IoT, IIoT, Power Systems
Network Virtualization	46	16	Mininet* (15), OpenvSwitch (OvS)*† (8), GNS3* (6), EXata network modelling* (3), NS3* (2), OpenDSS* (2), CORE* (1), Cooja† (1), EVE community edition† (1), MiniCPS* (1)	CPS, ICS, ICT, IoT, IIoT, Power Systems, RAN & Mobile Devices
Reverse-Proxy	1	1	Nginx Proxy Manager* (1)	ICT

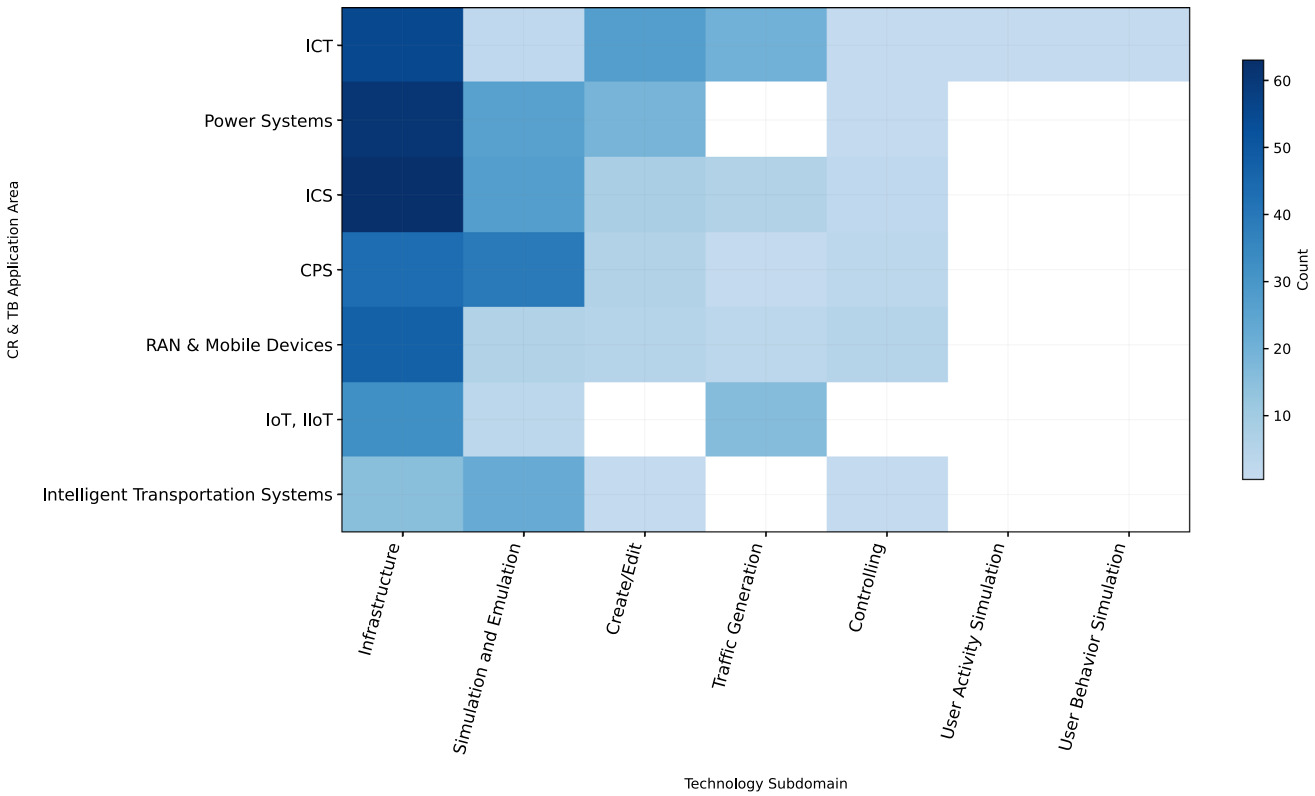


Fig. 17 Scenario Subdomain Distribution Across Cyber Range Application Areas

an engineering workstation, while a separate VM operates as a central log server to support an explainable, self-aware intrusion-detection and active-response framework for the grid [214]. In an ICS TB that reflects real-world power-system environments with HMIs, PLCs, power-quality monitors, and protocols such as Modbus, IEC 60870-5-104, and IEC 61850, Modbus appears among the core communication protocols used by a toolchain that automates attack-scenario generation around a common data model, enabling integration of real-world attack scenarios that emulate steps taken by manual penetration testers [13]. One study on protection IEDs highlights IEC 61850 GOOSE as a protocol that is vulnerable due to low-latency requirements, multicast packet delivery, and lack of encryption, and uses this protocol as the basis for evaluating how different commercial IED implementations respond to and recover from attacks in order to understand security implications of GOOSE-based communication [25]. A digital power-twin environment for smart grids employs GOOSE for time-critical communication between IEDs in the physical TB and in the digital twin, where GOOSE messages carry anomaly alerts and trigger immediate protective actions, enabling users to deploy real-world attacks and countermeasures and to study their effectiveness in a more easily modifiable and reproducible environment than a purely physical setup [74].

Simulation and Emulation

A co-simulation platform for power-distribution systems models the cyber layer in MATLAB/Simulink while the power system is represented in DIgSILENT PowerFactory, with real-time data exchange handled through a Matrikon Open Platform Communications (OPC) server and Distributed Network Protocol 3 (DNP3) communication modeled in dedicated software, so that model-based reinforcement learning can be used to detect coordinated cyber–physical attack events and infer attacker goals [153]. Another study on oscillatory load attacks initiated by exploited EV charging stations builds the IEEE New England 39-bus system in MATLAB/Simulink, using this system-stability model to synthesise benign and malicious datasets that underpin an edge-based detection and localisation approach combining cyber and physical features with deep-learning methods [155]. In a real-time co-simulation TB for the public EV charging ecosystem, the Opal-RT HYPERSIM simulator runs on a Windows VM connected to OP5650 real-time digital-simulator hardware to represent the power grid interlinked with EV infrastructure, providing real-time simulations that feed a monitoring platform for detecting EV-based cyberattacks [146]. A wide-area power-system application TB employs an OPAL-RT real-time digital simulator to host large-scale grid models and uses the IEC 61850 I/O interface of RT-LAB to map physical IEDs to the simulator, supporting efficient modelling of logical nodes in physical relays and enabling hardware-in-the-loop experiments with industry-grade devices [143].

Create/Edit

In a cyber-physical security simulation TB for power-system distribution networks, Modbus is characterised as a widely used client–server protocol in industrial automation, where SCADA systems in control centres act as Modbus clients that request information from remote terminal units as servers, and the resulting communications are used to analyse the impact of cyberattacks on distribution systems [170]. Another TB for evaluating attack-resilient network agents expands PLC capacity by attaching Modbus TCP devices so that additional slave PLCs can read from and write to the registers of a master PLC through a standardised addressing system, creating realistic control traffic patterns for experiments that initiate attacks leading to OT plant instability [140]. The Tectonic cyber range describes each scenario using a specification language based on YAML, where YAML files define machines, networks, and configurations applied to the scenario's machines, supporting customizable network configurations, real-time monitoring, and automated attack simulations that bridge theoretical knowledge and practical skills [64]. Within the CRACK framework, scenario design starts from theatre elements such as networks and compute nodes and progresses to scenario aspects such as vulnerabilities, with the entire scenario encoded in 2385 lines across 29 YAML files, so that the YAML-based scenario description language (SDL) provides a declarative way to specify elements and their interplay for design, model verification, generation, and automated testing of cyber scenarios [150].

Traffic Generation

In an SDN-based TB for defending against DDoS attacks launched by malicious IoT systems, curl-loader generates valid HTTP traffic while other tools create diverse DDoS request patterns, so that the mixture of legitimate and attack traffic can be used to evaluate a semi-supervised deep extreme learning machine and mitigation algorithm embedded in the SDN controller [141]. A hierarchical DDoS defence system for SDN environments also uses curl-loader to create flash-traffic workloads by simulating large-scale HTTP client requests, contributing to the SDN-DAD dataset that combines legitimate traffic, flash traffic, and various DDoS attacks for evaluating detection features that minimise computational load on the controller [77]. In an ICS TB that evaluates a dynamic and reliable intrusion-detection model, Acunetix is employed to generate network traffic throughout the TB, producing the web-traffic patterns against which the two-step classification and rejection-based reliability evaluation of network attacks are performed as the model adapts to evolving traffic [45].

Controlling

A CPS TB on the National Science Foundation (NSF) AERPAW platform integrates the Flower Framework to host a federated-learning scenario where a YOLOv8 model is deployed for object detection on edge devices such as drones, and the framework is used to study optimization and defence mechanisms like differential privacy and adversarial training for network incident anomaly detection under benign and variously poisoned conditions [85]. In a resilience-focused TB that models a truck with an autonomous cyber-defence system and physical resilience features, OpenTAP automates the execution of experiments and offers a GUI for configuring experiment steps, enabling repeatable and systematic runs that collect resilience-relevant data while the system is subjected to malware attacks [202].

User Activity Simulation A network-traffic–generation setup for CRs uses Selenium together with Python scripts to manipulate web pages through Firefox, where instances are equipped with the required browser add-on so that scripted actions can be issued easily via Selenium commands and contribute to realistic traffic that enhances the quality of training [50].

User behaviour Simulation In a log-data–oriented TB for cybersecurity experiments, Selenium remotely controls a Firefox browser window that is opened at the start of each session and closed afterwards, generating realistic and reproducible user interaction patterns that populate log datasets intended for intrusion-detection research with transparent, adaptable, and publicly available traces [188] (Table 10).

Table 10 Top-10 Technologies per Subdomain for Scenario. Superscripts: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration

Technology Subdomain	Total Mentions	Unique Tech.	Top-10 Technologies	Domains
Controlling	5	5	Flower Framework (1), OpenTAP‡ (1), RT-LAB* (1), SCORCH‡ (1), WebGME* (1)	CPS, ICT, Intelligent Transportation Systems, Power Systems
Create/Edit	45	28	Modbus (6), YAML‡ (6), JSON‡ (5), INET (2), RSCAD simulation software* (2), Totally Integrated Automation Portal Services (TIA Portal Services) (2), Apache SkyWalking (1), CSV (1), DIGSI 4 (1), GAMS* (1)	CPS, ICS, ICT, Intelligent Transportation Systems, Power Systems, RAN & Mobile Devices
Infrastructure	310	160	Modbus* (27), GOOSE* (12), MQTT* (11), OpenPLC (11), DNP3* (10), MMS* (7), OpenFlow* (6), Free5GC* (5), Ryu* (5), UERANSIM* (5)	CPS, ICS, ICT, Intelligent Transportation Systems, IoT, IIoT, Power Systems, RAN & Mobile Devices
Simulation and Emulation	120	67	MATLAB/Simulink* (12), Opal-RT Simulator* (8), OMNeT++* (6), SUMO* (5), Factory I/O* (4), Pandapower* (4), HYPERSIM* (3), RT-LAB* (3), RTDS simulator* (3), Unity3D* (3)	CPS, ICS, ICT, Intelligent Transportation Systems, Power Systems
Traffic Generation	19	18	curl-loader (2), Acunetix (1), Apache Bench (1), Arachni (1), BUP - Benign User Profiler (1), D-ITG (1), Locust (1), Mouseworld testbed (1), Nessus (1), Nmap (1)	ICS, ICT, IoT, IIoT, RAN & Mobile Devices
User Activity Simulation	1	1	Selenium (1)	ICT
User behaviour Simulation	1	1	Selenium (1)	ICT

5 Discussion

This chapter first critically reflects on the challenges encountered when conducting this work and discusses methodological limitations. It then analyses characteristic patterns and trends in the collected repository of information. Finally, it answers the research questions from Section 1.

5.1 The challenges of categorization and terminology

Related surveys highlight ongoing issues in the literature regarding taxonomies and conceptualizations of cyber ranges and testbeds. For example, terminology and taxonomies differ across publications and existing taxonomies are not used consistently. However, the architectures and terminologies used in the surveys themselves also differ considerably. The following table 11 present the architectures and key terms used in these surveys. While a tabular representation does not capture the full complexity of the architectures, it is sufficient to highlight the main differences. The first column lists the comparison category, while the following three columns describe the corresponding categories and their subcategories in parentheses (Table 11).

Table 11 compares the architectures and their terminologies. The first column lists the comparison category, while the following three columns describe the corresponding categories and their subcategories in parentheses.

All architectures include an entry point or user access mechanism, but they use different names and levels of detail. According to [71], administration and orchestration of exercises include user and asset management as well as scheduling. In the publication by [189], no dedicated layer or zone is defined for this purpose. Instead, related features are described within the cyber range capabilities, such as reporting, training methods, and data collection. In the architecture proposed by [208], these aspects are covered by the category *Management*. Furthermore, [208] describes a testing module that is not included in the other two architectures. For orchestration and provisioning (e.g., infrastructure as code (IaC) and APIs) as well as for the virtualization or infrastructure layer, [189] and [71] define separate categories, whereas [208] combines these aspects and does not explicitly mention orchestration. A data or storage layer is only

Table 11 Crosswalk comparison of logical cyber range architectures (simplified)

Comparison category	Kampourakis et al. (2025) [71]	Ukwandu et al. (2020) [189]	Yamin et al. (2020) [208]
User access / entry point	Control Access Zone (authentication, authorization)	Users; Front-End Technologies (web browsers, web server tech)	Portal (user, admin, client)
Administration / orchestration of exercises	Management Zone (scheduling, user/asset mgmt, data analysis)	Cyber Range Capabilities(scenarios, reporting, training methods, data collection mechanism)	Management (cyber range, scenario, exercise/test)
Monitoring / scoring / reporting	Monitoring Zone (monitoring, data collection/analysis, scoring/reporting)	Cyber Range Capabilities (reporting, data collection mechanism)	Monitoring (collection, analysis, logging); Training & Education (scoring, after-action analysis)
Scenario lifecycle / content authoring	Learning Management and Support Zone (scenario development, automation, traffic generation)	Cyber Range Capabilities (scenarios)	Scenario (create/edit, deploy, generate, execute, control, destroy)
Training / pedagogy support	Learning Management and Support Zone (TTPs, traffic capture)	Cyber Range Capabilities (training methods, gamification, visualisation)	Training and Education Module (tutoring, scoring, after-action analysis)
Testing / validation module	-	-	Testing Module (test case definition, analysis & verification)
Virtualization / infrastructure layer	Core Infrastructure Zone: Underlying infrastructure (servers, network Devices, security functions, software & services, storage, computers & mobile Devices); Virtualization (aWS, OpenStack, vSphere, Docker)	Core Technologies (emulation, virtualisation, simulation, containerisation)	Run-time Environment (emulate, simulate, traffic/attack generation, HW, user behaviour generation)
Orchestration / provisioning (IaC / APIs)	Core Infrastructure Zone: Orchestration (Kubernetes, Terraform, Ansible, API etc.)	Infrastructure Technologies: Orchestration (e.g., vSphere; Wisper; etc.)	-Run time Environment (deployment, controlling); (orchestration not explicitly named)
Data / storage layer	Underlying Infrastructure (Storage)	-	Data Storage (scenario definitions, rules, tools, replica data, parameters)

described by [71] as a feature or capability within the underlying infrastructure. A dedicated *Data Storage* category is provided only by [208], while [189] does not explicitly mention this aspect. The remaining comparison categories appear in all architectures, but they differ in content, terminology, and their placement within the overall architecture. In addition, the publications analysed to build the data repository of this work do not apply these terms and reference architectures consistently. For example, Chouliaras et al. [37] group virtual machines and cloud services into an "environment" component, place infrastructure containerization and orchestration technologies such as Docker, YAML, or Ansible under "scenario," and assign development tools such as VSCode to orchestration. Another example is [64], which separates orchestration tools and an IaC layer, and describes a presentation layer that includes heterogeneous tools such as Moodle, Kibana, and MITRE Caldera. The differences in architectures and terminology, missing categories for cyber range features in existing architectures, and the inconsistent use of terms and architectural representations across the analysed publications created a major challenge for a comprehensive and objective clustering and categorization of all features and technologies. Our approach was that we collected relevant terms from the analysed publications and grouped them into categories whose labels reflect the shared semantic meaning of the assigned terms. This approach inevitably involves subjective interpretation decisions, and alternative categorizations and mappings are therefore possible. Having illustrated the variability in terminology and architectural representations, we now analyse quantitative patterns in the extracted repository, focusing on gaps, anomalies, and trends across *application areas*, *purposes*, and *technology domains*.

5.2 Gaps, anomalies, and trends in the data repository

The following findings are derived from technologies and classifications *reported* in the reviewed publications. Therefore, observed gaps should be interpreted as "absence in the analysed corpus" and may also reflect publication and reporting practices rather than the absence of such technologies in real-world deployments.

Across all *application areas* (Fig. 18), the *technology domain Scenario* is the most frequently represented (578), followed by *Red Team Operations* (315) and *Computing Platform* (193). Exact contents are described in Section 4.3. Several *application areas* show a more concentrated profile. In *Power Systems*, most technologies are assigned to the *Scenario* domain (107), while other domains have substantially lower values. ICS also shows peak values in *Scenario* (108) and *Red Team Operations* (71), but remains lower in other domains. This indicates that some *application areas* rely on a narrower set of *technology domains*, whereas others (in particular ICT) show a broader distribution of reported technologies. Domains with lower overall intensity, such as *Data Storage* (35), *Management* (31), and *Portal Services* (34), are still sparsely represented. We also observe explicit gaps where no technologies are reported for specific application-area/domain combinations (e.g., CPS *Management*, CPS *Portal Services*, Intelligent Transportation Systems *Network Infrastructure*, Intelligent Transportation Systems *Portal Services*, and RAN & Mobile Devices *Management*). Regarding the distribution of CRs and TBs across *application areas*, CRs are more frequently used in ICT than in other areas. A notable pattern is the frequent use of CRs in combination with the *Training and Exercises* and *Education purposes*, particularly in ICT and ICS (Figure 4). Overall, this distribution suggests a functional separation: dedicated TBs are reported more frequently for *Research, Testing and Experimentation*, whereas CRs are reported more frequently for *Training and Exercises* and *Education*. At the same time, several of the other *application areas* show an increase in publications, especially within the last two years (Figure 3). Within *Research, Testing and Experimentation*, the most common *use cases* are *Threat and Vulnerability Assessment*, *Attack Impact Assessment*, and *Dataset Generation*, and dedicated TBs are used particularly often. This use-case profile suggests that experimentation-oriented settings emphasize assessment- and data-driven activities. Only for the *use case Traffic Generation* are CRs mentioned more frequently than TBs (Figure 5), indicating that CRs may be preferred when traffic generation is embedded in a broader scenario context rather than treated as an isolated testbed task. In *Training and Exercises use cases*, the use of TBs is less pronounced, and CRs are more dominant. Besides general security training (covering training mentions without a specific thematic focus), CTF, *Incident Response*, and *Red vs. Blue Team* trainings are particularly prominent (Figure 6), which suggests that interactive and exercise-oriented *use cases* are more frequently realised through CRs in the reviewed corpus. In the *Education purpose*, CRs also dominate. Here, *Student Assessment & Scoring*, *Learning Management Systems*, and *Instructional Design use cases* are mentioned most frequently (Figure 7), indicating a strong emphasis on structured course integration and evaluation mechanisms.

In the following, we analyse temporal trends in the cyber range and testbed literature to examine how reported *use cases* and technologies evolve over time. We focus on quarterly developments and use normalized shares to mitigate the overall increase in publication volume in 2024–2025. The three small-multiple figures visualize quarterly time series of normalized use-case shares within each *purpose* (*Research, Testing and Experimentation*, *Training and Exercises*, and *Education*) and refer to the top-10 *use cases* per *purpose* reported in Section 4.2. Because some quarters contain only a small number of publications, the normalized curves are occasionally spiky and may reach 100%. In these cases, the dashed count curves help distinguish substantive increases from low sample sizes and from shifts in the quarter's overall publication volume within the respective *purpose*.

In *Research, Testing and Experimentation* (Figure 19), the profile shifts from an early dominance of *Threat and Vulnerability Assessment* and *Attack Impact Assessment* toward a more diversified pattern in 2024–2025, where *Dataset Generation* becomes more prevalent and *Cyber Security Resilience Assessment* gains prominence. In the same period, additional solution-oriented and ML-related topics become visible and increase in frequency (e.g., *Mitigation Strategies* and *ML-based IDS/IPS*), while *Traffic Generation* remains sporadic. For *Training and Exercises* (Figure 20), the emphasis shifts toward hands-on training formats, with *Capture the Flag* and *General* training dominating the later period, whereas earlier team-based and specialized formats (e.g., *Red Team vs. Blue Team*) are no longer reported in the recent quarters. In *Education* (Figure 21), *Student Assessment & Scoring* and *Learning Management Systems* remain the most consistently reported use cases. Assessment and scoring becomes relatively more prominent in 2024–2025. *Learning Labs* appears only in the later period, while *Instructional Design* becomes comparatively less dominant.

5.2.1 Technologies

In the *technology domain Red Team Operations*, subdomain *Adversary Emulation*, only a small number of tools are used, namely MITRE Caldera and Infection Monkey. Other tools are not reported in the publications that perform adversary emulation, or the activities are implemented manually (Section 4.3.1). This limited set suggests a low diversity of

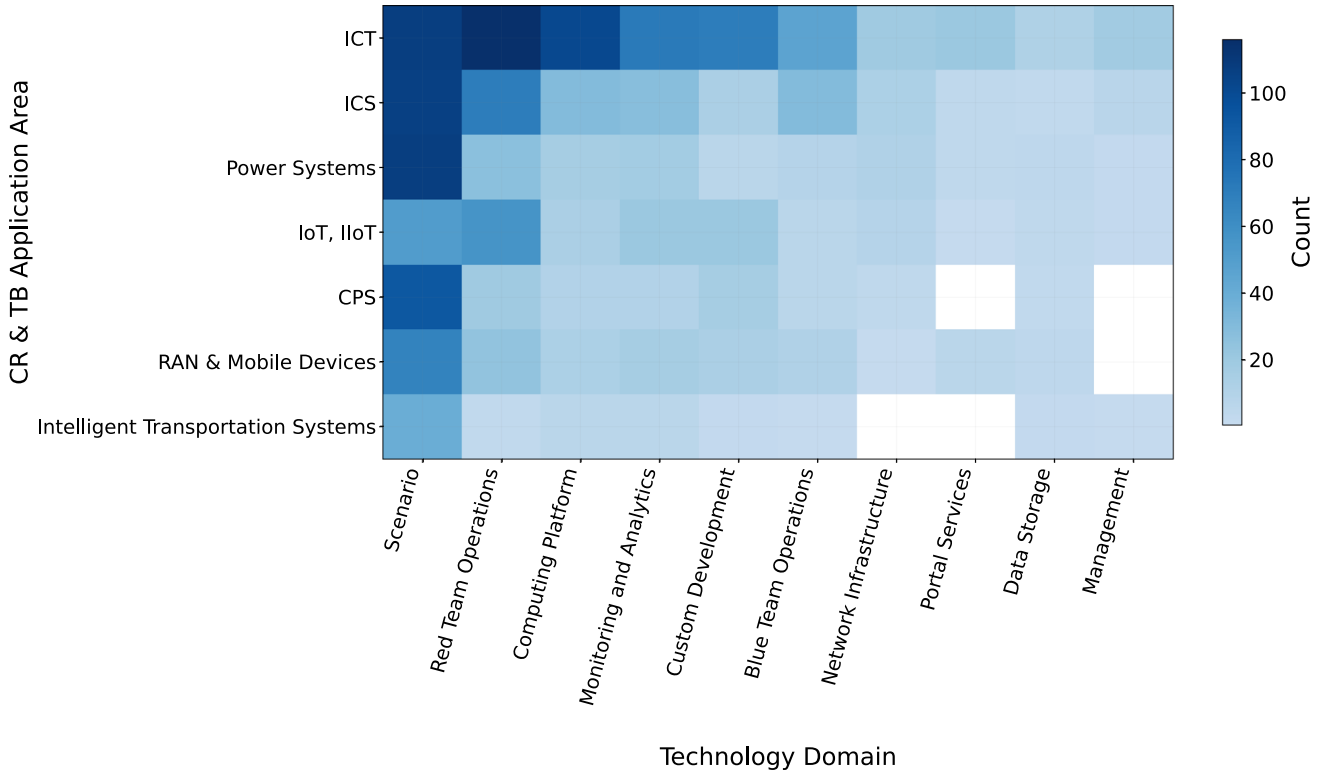


Fig. 18 Technology Distribution Across Cyber Range Application Areas

reported tooling for adversary emulation in CR/TB implementations and may indicate that adversary emulation is either less frequently implemented as an explicit capability or is implemented without dedicated tools and therefore less consistently documented. Metasploit can also be used for adversary emulation [88], but in the analysed publications it is primarily used as a penetration testing tool or for executing individual attacks (Section 4.3.1). This example illustrates that technology classification depends on the described usage context rather than on the general capabilities of the tool. A similar rationale is applied in Section 4.3.1, where SQL databases are used only as targets for SQL injection exercises and are therefore assigned to the category *Red Team Operations*, specifically under *Training and Practice Systems*. In the *Containerization* subdomain, Docker is used almost exclusively. Only Podman is mentioned once as an alternative, indicating that Docker is reported as a de facto standard for containerization in the reviewed CR/TB implementations. The subdomain *Software Provisioning and Configuration* also contains only two tools across all reviewed publications: Ansible and AWX, which provides a web-based user interface, REST API, and task engine for Ansible (Table 4), suggesting that provisioning and configuration tasks are similarly dominated by a small set of mature, widely adopted tools. Further subdomains that contain only a single mentioned technology include *Application Security Testing* (Contrast Security), *Incident Management & Response* (TheHive), *Security Hardening* (CIS Ubuntu Security Guide), *Honeypot Systems* (honeyD) and *Reverse-Proxy* (Nginx Proxy Manager), which indicates limited reported coverage for these feature areas within the analysed corpus. The *technology domain Custom Development* also contains technologies that appear only once across all publications. Because this domain often reflects implementation stacks such as libraries and frameworks rather than CR/TB-specific building blocks, we treat it separately and do not discuss it further here.

5.3 Technological evolution of cyber ranges and testbeds

While a fine-grained temporal trend analysis of individual technologies is limited by inconsistent reporting practices across publications, a comparison at the level of technology domains and dominant tools with the findings of earlier surveys is nonetheless informative, as these works employ explicit tool inventories that allow for meaningful cross-survey comparison.

Regarding the computing platform, Yamin et al. [208] and Ukwandu et al. [189], whose publication sets extend to 2019–2020, identify hypervisor-based virtualisation as dominant, with VMware cited most frequently, while containerisation

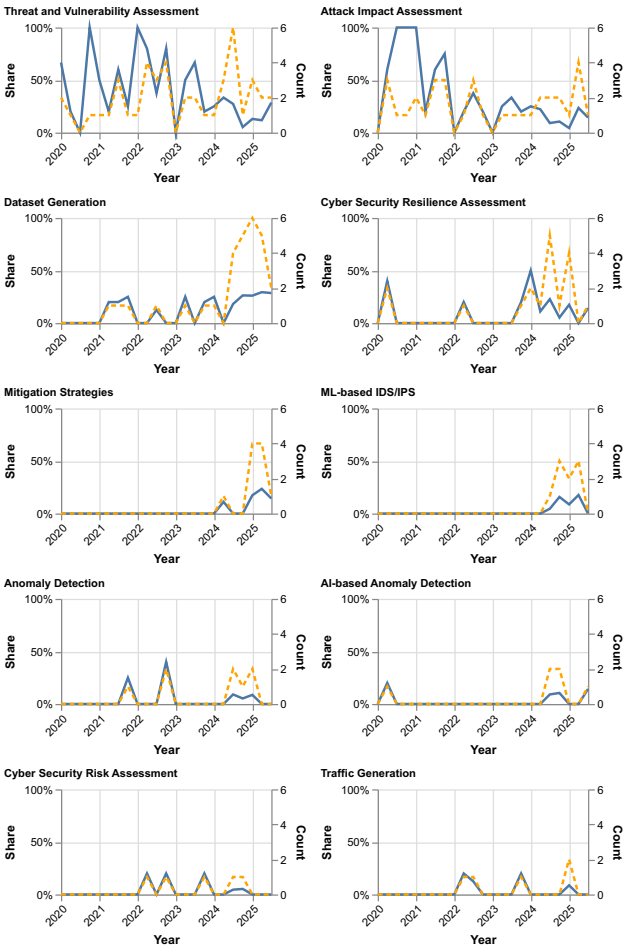


Fig. 19 Trends in "Research, Testing, and Experimentation" Purpose

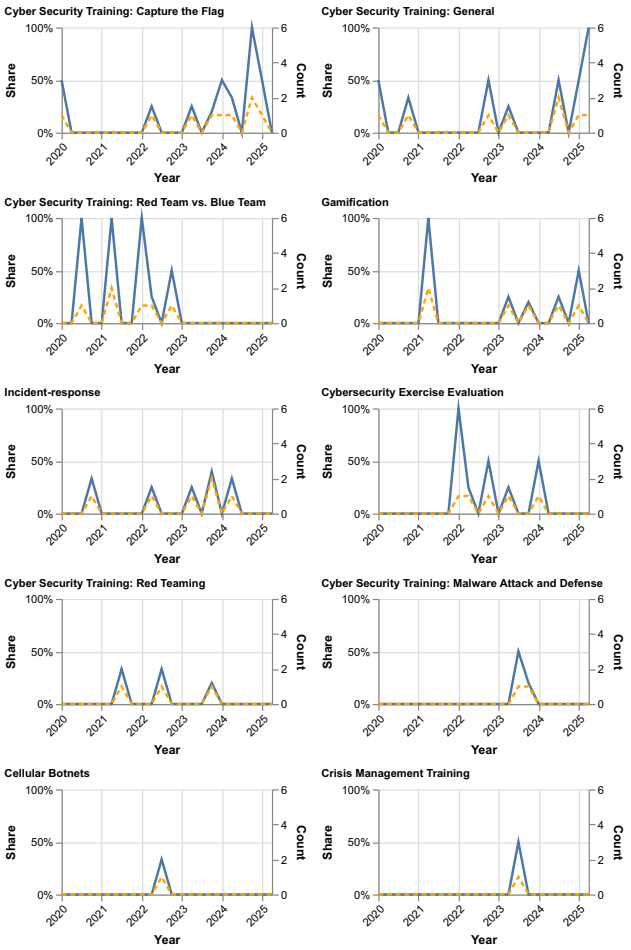


Fig. 20 Trends in "Training and Exercises" Purpose

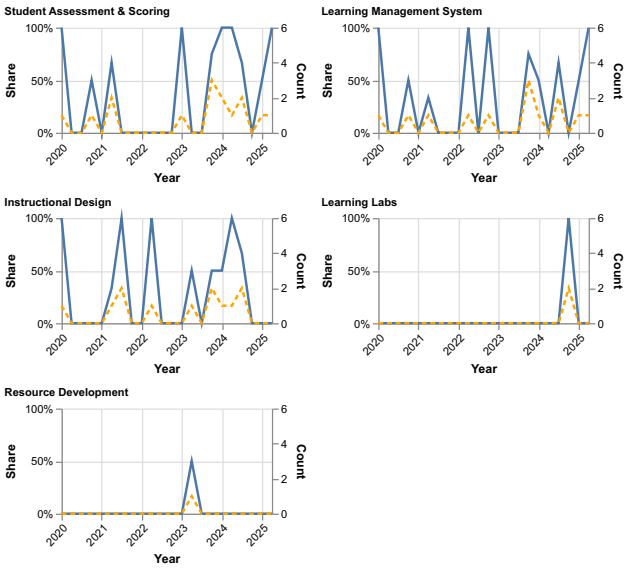


Fig. 21 Trends in "Education" Purpose

is introduced as a lightweight and scalable complement to VM-based approaches. The present survey indicates a clear shift: Docker is the most frequently reported containerisation technology (34 mentions), whereas traditional hypervisors remain present but no longer exclusive, with VMware vSphere (9), KVM (5), and VirtualBox (11) coexisting alongside container-based deployments. This coexistence pattern is consistent with the findings of Kampourakis et al. [71], who identify the combination of hypervisor-2, container-based, and private cloud virtualisation as the most common configuration in CR implementations up to 2023.

In the domain of orchestration, earlier surveys describe infrastructure management primarily in terms of virtualisation layers [189] or scenario execution modules [208], without identifying a dominant set of dedicated provisioning tools. Chouliaras et al. [38] and Kampourakis et al. [71] mark a progression toward explicit IaC tooling, with the present survey confirming Ansible (12 mentions) and Terraform (7 mentions) as the leading solutions and Kubernetes (4 mentions) establishing container orchestration as a recognisable architectural category.

In red team operations, Metasploit (23 mentions) and Nmap (31 mentions) remain the dominant tools for exploitation and network scanning respectively, consistent with their prominence in earlier literature [208]. The main development is the emergence of framework-level tooling: MITRE ATT&CK (6 mentions) and MITRE Caldera (4 mentions) represent a shift toward structured, framework-guided adversary emulation that is not present in any of the earlier surveys.

The scenario domain shows the strongest continuity: MATLAB/Simulink (12 mentions), OPAL-RT simulators (8 mentions), and industrial protocols such as Modbus (27 mentions) and GOOSE (12 mentions) remain foundational across ICS and power systems scenarios throughout the period, reflecting stable domain-specific infrastructure requirements.

Finally, AI and ML frameworks such as TensorFlow (12 mentions), Keras, and Scikit-learn represent a technology domain with no direct counterpart in the earlier surveys. While this absence may partly reflect differences in scope and categorisation between surveys, it is consistent with the broader integration of machine learning into cybersecurity research workflows observed in the 2020–2025 period.

5.4 Answering the research questions

Building on these observations, we now answer the research questions introduced in Section 1. *RQ1: What use cases and application areas for cyber ranges (CRs) and testbeds (TBs) are reported in the literature?*
In our literature review, we identified the following *application areas*: ICT, ICS, CPS, IoT/IIoT, RAN & Mobile Devices, Power Systems, and Intelligent Transportation Systems. Section 4.2 provides a more detailed list of *use cases*, organised under the CR/TB *purposes Research, Testing and Experimentation*, *Training and Exercises*, and *Education*. Table 12 summarizes the top three *use cases* per *purpose*, ranked by the number of articles.
RQ2: Which technologies and technology groups are used to implement specific CR/TB features?
Table 13 presents the most frequently reported technologies for selected *technology subdomains* related to the *use cases* shown in RQ1. We use *Technology Subdomains* as a proxy for CR/TB features, because the more fine-grained category *Technology Functionality* primarily describes the specific functionalities of individual tools. In contrast, the *Technology Subdomain* category groups multiple tools with similar functionalities and therefore best represents CR/TB "features" at an appropriate level of abstraction. The table shows a wide variety of technologies, including tools, protocols, virtualization technologies, databases, and data formats. It includes well-established technologies with many mentions in the analysed publications, such as Metasploit (23) in the subdomain *Exploitation and Attack Execution*, Docker (34) in the subdomain *Containerisation*, and protocols such as Modbus (28), which is frequently described in publications in the ICS domain as an essential part of the scenario infrastructure or for attack execution. At the same time, the table also reveals less well-covered categories, such as Management or certain database categories, which include fewer than three distinct tools and fewer than ten total mentions. The detailed results are provided in Section 5.2.
RQ3: What trends and notable patterns can be observed in the research and development of cyber ranges and testbeds (e.g., purposes, application areas, and technologies)?
In Section 5.2, we first report the peak values of *technology domains* across the entire data repository, ranked by the number of mentions, namely *Scenario*, *Red Team Operation*, and *Computing Platform*, as well as peak values in the less frequently represented *application areas*. In addition, we analysed the usage frequency of cyber ranges and testbeds. The results show that cyber ranges are used most frequently in the ICT *application area*, and in particular in ICT for *Training, Exercises, and Education*. Furthermore, we highlight notable patterns in the technology landscape. This includes both underexplored areas, such as the use of tools for adversary emulation, and well-established technologies used in CRs and TBs, such as Docker and Ansible.

6 Future work

The remaining section discusses aspects future surveys should address based on the systematic literature review at hand. Furthermore, the section points out future trends related to the emergence of AI.

6.1 Taxonomic harmonization and semantic formalization

The challenges identified in the discussion in Section 5 with regard to taxonomies and logical architectures not only indicate an existing research gap, but also underscore the necessity of a shared conceptual foundation in this domain. Against this background, it appears essential that future work systematically advances existing taxonomies and architectures while applying them consistently to established architectural descriptions, documentation, and taxonomic frameworks. Such harmonization can substantially facilitate the planning, design, and classification of CRs and TBs and, moreover, support the targeted further development of CRs and TBs with respect to their architecture, functionality, and integration.

The heterogeneous terminology and architectural representations identified throughout this survey suggest that reproducibility and comparability in CR and TB implementations cannot be achieved through procedural tooling alone.

Table 12 Top-3 use cases per purpose, ranked by the number of articles.

Purpose	Top 1	Top 2	Top 3
Education	Student Assessment & Scoring (14)	Learning Management System (12)	Instructional Design (11)
Research, Testing and Experimentation	Threat and Vulnerability Assessment (46)	Attack Impact Assessment (35)	Dataset Generation (29)
Training and Exercises	Cyber Security Training: Capture the Flag (9)	Cyber Security Training: General (8)	Cyber Security Training: Red Team vs. Blue Team (6)

Ontology-based approaches represent a promising direction for establishing such a foundation. Wen et al. [203] propose an RDF/OWL-based ontology for modelling cyber security exercise scenarios, providing a common semantic structure that enables scenario knowledge to be shared and reused across applications and community boundaries. Building on this, Kampourakis et al. [73] propose a broader ontology-based framework that formalizes the structural, functional, informational, and decisional aspects of the entire CR ecosystem into a machine-interpretable model implemented in OWL 2 DL, enabling consistency checking, automated reasoning, and traceability across abstraction levels. The authors characterize this framework as a semantic meta-model over architectural knowledge, addressing precisely the kind of terminological and representational heterogeneity identified in this survey. The structured data repository assembled here, consolidating technologies, use cases, and architectural layers across 199 publications, may serve as empirical input for such formalization efforts, and future work could build on this foundation to develop shared, semantically grounded representations of the CR and TB domain.

With respect to the methodology of this work, the semantic summarization and categorization of technologies allows for a comparatively large degree of interpretative latitude. A more structured approach that relies on qualitative analysis and the explicit identification of individual technological functions ultimately appears methodologically more suitable, as these functions constitute the features of CRs and TBs. Future research could examine and qualitatively evaluate individual components of this work in greater depth in order to derive an alternative categorization and structuring that is more precise and better aligned with the context.

6.2 Generative AI and large language models

A further trajectory concerns the integration of generative AI and large language models (LLMs) into CR and TB implementations. The AI and ML technologies identified in this survey are predominantly applied for detection and analysis tasks, such as anomaly detection and intrusion detection model training. Generative AI represents a qualitatively different direction: Zacharis and Patsakis [212] propose an ML-assisted framework for automated cyber exercise content generation using named entity recognition and a dedicated scenario ontology, while Palumickas et al. [128] evaluate a generative AI prototype for dynamic, interactive scenario generation and demonstrate both its potential and current limitations regarding consistency and repeatability. Yamin et al. [209] explore the use of LLMs as active participants in exercise simulations rather than merely as scenario authoring tools, and Kampourakis et al. [72] demonstrate the use of LLM-assisted expert reasoning to support structured CR evaluation. Berg et al. [15] demonstrate that LLMs can automate the generation of runnable ICS simulations from plain-language descriptions, producing functioning testbeds in under 90 seconds, and argue that such prompt-to-simulation pipelines are well-suited for CRs, deception systems, and rapid prototyping, even though the generated models are not suitable for high-fidelity simulations. Given that these works largely postdate the corpus examined in this survey, the systematic integration of generative AI into CR and TB workflows, including scenario generation, automated red teaming, and platform evaluation, represents a critical emerging trajectory for future research.

6.3 Further platforms and directions for targeted surveys

The systematic scope of this survey means that several representative platforms documented in the literature fall outside the analysed corpus. Sipola et al. [168] describe a digital twin of a food supply chain deployed on the Realistic Global Cyber Environment (RGCE) platform operated by JAMK University of Applied Sciences, demonstrating its use in a live cyber exercise for training organizations in supply chain cybersecurity. Bonagura et al. [26] introduce the Hydra testbed, which emulates a real-world water distribution system and is used to generate the HydraCPS dataset for evaluating intrusion detection systems under simulated cyber-physical attacks on critical infrastructure. Cruz and Simões [42] describe a flexible framework for the creation of laboratory and ICS cyber range environments for training purposes, applied in the context of a course on cyber-physical systems security. The iTrust testbeds at the Singapore University of Technol-

Table 13 Top-3 technologies per selected technology subdomain

Technology Subdomain	Top 1	Top 2	Top 3
Infrastructure	Modbus (28)	GOOSE (12)	MQTT (11)
Network Scanning and Reconnaissance	Nmap (31)	Wireshark (7)	MulVAL (3)
Exploitation and Attack Execution	Metasploit (23)	Ettercap (8)	Sqlmap (6)
Containerisation	Docker (34)	Podman (1)	nan
Network Virtualization	Mininet (16)	OpenvSwitch (OvS) (8)	GNS3 (6)
Cloud Infrastructure	OpenStack (19)	Amazon Web Services (AWS) (8)	Google Cloud (2)
Simulation and Emulation	MATLAB/Simulink (12)	Opal-RT Simulator (8)	OMNeT++ (6)
Data Collection	Wireshark (13)	Tcpdump (7)	scapy (3)
Intrusion Detection & Prevention (IDS/IPS)	Snort (11)	Suricata (9)	Zeek (3)
AI & Machine Learning	TensorFlow (12)	Keras (4)	Scikit-learn (4)
Analysis & Verification	Wireshark (12)	ScadaBR (4)	Tshark (4)
Virtualization platform/Type-2-Hypervisor	VirtualBox (11)	VMWare Workstation (6)	QEMU (3)
Training and Practice Systems	Apache web server (7)	Modbus (7)	DVWA (5)
Create/Edit	Modbus (6)	YAML (6)	JSON (5)
Visualization & Dashboarding	Kibana (9)	Grafana (6)	Matplotlib (2)
Relational Database	MySQL Database (8)	SQLite (4)	PostgreSQL (2)
User Access	OpenSSH (7)	Apache Guacamole (3)	Virtual network computing (VNC) (3)
Dataset Generation	CSV (10)	Apache Bench (1)	Apache Flume (1)
SIEM & Security Analytics	Security Onion (4)	Wazuh SIEM (4)	ELK Stack (2)
Vulnerability Management	Owasp Zap (Zed Attack Proxy) (4)	Nikto (3)	OpenVAS (3)
Firewall and routing platform	PfSense (5)	OPNSense (3)	IPFire (1)
Integrated Development Environment	Jupyter notebook (3)	FUXA (2)	Node-RED (2)
Identity & Directory Services	Windows Active Directory (5)	Security Credential Management System (SCMS) (1)	nan
NoSQL Database	MongoDB (4)	AWS NoSQL DB (1)	Amazon DynamoDB (1)
Time-series database	InfluxDB (4)	PingThings' Berkeley Tree Database (BTrDB) (1)	nan
Admin Access	Apache Guacamole (2)	OpenSSH (2)	nan
Asset & Infrastructure Management	Dragos OT Asset Visibility and Inventory (1)	GIT (1)	Windows Active Directory (1)
Platform & Environment Management	9p (1)	LAMP stack (1)	OpenPLC (1)
Identity & Access Management (IAM)	OAuth 2.0 (1)	Windows Active Directory (1)	nan
Reverse-Proxy	Nginx Proxy Manager (1)	nan	nan

ogy and Design [167], including SWaT, WADI, and EPIC, are well-documented OT security research environments. None of these platforms were retrieved by the applied search protocol, as the corresponding publications appeared in sources outside the three searched databases or were referenced primarily through institutional repositories. A targeted survey of integrated and domain-specific CR and TB platforms represents a valuable direction for future work.

7 Conclusion

This survey examined how CRs and security TBs are implemented in practice by focusing on the *technologies* used to realise CR/TB scenarios and features. Building on a systematic literature review across 2020–Aug. 2025, we included 199 publications and consolidated the extracted *application areas*, *purposes*, *use cases*, infrastructure types, and reported technologies into a structured data repository for analysis.

Within this repository, we identified 650 distinct technologies and mapped them into a hierarchical taxonomy with 10 *Technology Domains* and 81 *Technology Subdomains*, enabling consistent cross-paper comparison despite heterogeneous terminology and architectural representations. The repository further captures CR/TB *purposes* and *use cases* across *application areas*. *Research, Testing and Experimentation* is the most frequently represented *purpose*, and the literature suggests a functional separation in reported deployments: TBs are reported more frequently for experimentation-oriented *use cases*, whereas CRs are reported more frequently for *Training and Exercises* and *Education*.

It is important to note that this separation reflects patterns in *reported deployments and publication focus* rather than an inherent technical limitation of either platform type. As noted in Section 3, individual publications may address multiple purposes, and the core technology stack reported across CR and TB implementations is largely shared throughout the corpus (see Section 4.3).

On the technology level, the *Scenario* domain is most frequently represented, followed by *Red Team Operations* and *Computing Platform*. Several *application areas* show concentrated profiles and explicit domain/application-area gaps, and the observed temporal trends indicate an increasing diversification of reported *use cases* in 2024–2025.

Based on the patterns observed in the data repository and the challenges discussed regarding inconsistent terminology and categorization across the literature, we recommend that future CR/TB publications report technologies and feature implementations more systematically (e.g., explicitly stating which components are implemented, how they are integrated, and which tools operationalize specific features). We further recommend adopting shared terminology and providing explicit mappings to reference architectures or taxonomies when describing CR/TB capabilities, to reduce ambiguity and improve comparability across studies.

A Appendix

The following list enumerates all extracted technologies, including additional information for categorization, cyber range or testbed classification, and the respective publications. Each technology extracted per publication is listed individually, which may result in multiple entries for the same technology. Due to space constraints, the list has been significantly abbreviated. Certain details have been omitted, including the technology's intended purpose, technology type (e.g., tool, protocol, data format), fine-grained functional categories of the technology within the cyber range or testbed, descriptions of technology *use cases*, subcategories of the cyber range *application area*, cyber range *use cases*, and article-related information.

The list includes the following columns:

- **Technology Name** (Technology)
- **Technology Domain** (TD)
- **Technology Subdomain** (TSD)
- **Cyber Range or Testbed Purposes** (CR/TB P I–III)
- **CR/TB**, indicating whether the publication describes a cyber range (CR) or a testbed
- **Source**, providing the reference for the publication
- **Date**, indicating the publication date of the source

Note: The **CR/TB P I–III** column uses the following abbreviations: **Education (E)**, **Research, Testing and Experimentation (RTE)**, and **Training and Exercises (TE)** (Tables 14, 15, 16, 17, 18, 19, and20).

Table 14 Data repository (Part 1/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Docker	Computing Platform	Containerisation		RTE		TB	2025-03	[7]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2025-03	[7]
MySQL Database	Red Team Operations	Training and Practice Systems		RTE		TB	2025-03	[7]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[7]
OAI 5G core	Scenario	Simulation and Emulation		RTE		TB	2025-03	[7]
OAIs gNB emulator	Scenario	Infrastructure		RTE		TB	2025-03	[7]
DETERLab	Computing Platform	Integrated Testbed Solutions		RTE		TB	2022-12	[156]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2022-12	[156]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2022-12	[156]
Modbus	Scenario	Create/Edit		RTE		TB	2022-12	[156]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2022-12	[156]
PowerWorld	Scenario	Simulation and Emulation		RTE		TB	2022-12	[156]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		TB	2022-12	[156]
Zabbix	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2022-12	[156]
GOOSE	Scenario	Infrastructure		RTE		TB	2025-07	[70]
IEC61850 open server	Scenario	Infrastructure		RTE		TB	2025-07	[70]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-07	[70]
Proxmox VE	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-07	[70]
RSCAD simulation software	Scenario	Create/Edit		RTE		TB	2025-07	[70]
RTDS simulator	Scenario	Simulation and Emulation		RTE		TB	2025-07	[70]
SV	Scenario	Infrastructure		RTE		TB	2025-07	[70]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-07	[70]
CICFlowMeter	Monitoring and Analytics	Data Collection		RTE		TB	2024-10	[65]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-10	[65]
GOOSE	Scenario	Infrastructure		RTE		TB	2024-10	[65]
IEC 60870-5-104	Scenario	Infrastructure		RTE		TB	2024-10	[65]
Sampled Values	Scenario	Infrastructure		RTE		TB	2024-10	[65]
Tcpdump	Monitoring and Analytics	Data Collection		RTE		TB	2024-10	[65]
Tshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-10	[65]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
VyOS	Network Infrastructure	Network Virtualization		RTE		TB	2024-10	[65]
MANO	Computing Platform	Infrastructure Provisioning and Configuration				TB	2023-07	[62]
OpenStack	Computing Platform	Cloud Infrastructure				TB	2023-07	[62]
Apache Kafka	Scenario	Infrastructure		RTE	TE	CR	2022-06	[145]
Elastic Logstash	Monitoring and Analytics	Log Management		RTE	TE	CR	2022-06	[145]
Elasticsearch	Data Storage	NoSQL Database		RTE	TE	CR	2022-06	[145]
Esper	Scenario	Infrastructure		RTE	TE	CR	2022-06	[145]
JSON	Scenario	Create/Edit		RTE	TE	CR	2022-06	[145]
Kafka SQL	Scenario	Infrastructure		RTE	TE	CR	2022-06	[145]
Keras	Custom Development	AI & Machine Learning		RTE	TE	CR	2022-06	[145]
MATILDA testbed	Scenario	Create/Edit		RTE	TE	CR	2022-06	[145]
Mouseworld testbed	Scenario	Traffic Generation		RTE	TE	CR	2022-06	[145]
Siddhi	Scenario	Infrastructure		RTE	TE	CR	2022-06	[145]
TensorFlow	Custom Development	AI & Machine Learning		RTE	TE	CR	2022-06	[145]
GOOSE	Scenario	Infrastructure		RTE		TB	2023-06	[25]
libIEC61850	Scenario	Infrastructure		RTE		TB	2023-06	[25]
Tshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-06	[25]
Common Industrial Protocol (CIP)	Scenario	Infrastructure		RTE		TB	2024-07	[33]
Rockwell Automations FactoryTalk Linx software	Scenario	Infrastructure		RTE		TB	2024-07	[33]
Rockwell studio 5000 logix designer software	Scenario	Create/Edit		RTE		TB	2024-07	[33]
Western Services Corporation (WSC) Generic Pressurized Water Reactor (GPWR)	Scenario	Simulation and Emulation		RTE		TB	2024-07	[33]
WSC 3keymaster	Scenario	Simulation and Emulation		RTE		TB	2024-07	[33]
Modbus	Scenario	Infrastructure		RTE		TB	2020-04	[67]
MulVAL	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2020-04	[67]
Siemens windows control centre (WinCC)	Red Team Operations	Training and Practice Systems		RTE		TB	2020-04	[67]
DIGSI 4	Scenario	Create/Edit		RTE		TB	2024-08	[4]
EMTP-ATP	Scenario	Simulation and Emulation		RTE		TB	2024-08	[4]
ETAP software	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-08	[4]
aireplay-ng	Red Team Operations	Paketmanipulation		RTE		TB	2024-12	[132]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Airgeddon	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[132]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2024-12	[132]
AWS Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2024-12	[132]
AWS NoSQL DB	Data Storage	NoSQL Database		RTE		TB	2024-12	[132]
Azure Digital Twins	Computing Platform	Cloud Infrastructure		RTE		TB	2024-12	[132]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-12	[132]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[132]
Google Colab	Custom Development	AI & Machine Learning		RTE		TB	2024-12	[132]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-12	[132]
MySQL Database	Scenario	Infrastructure		RTE		TB	2024-12	[132]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[132]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[132]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[132]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[132]
Cewl	Red Team Operations	Brute force attacks		RTE		TB	2021-05	[111]
CSV	Custom Development	Dataset Generation		RTE		TB	2021-05	[111]
DVWA	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[111]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2021-05	[111]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-05	[111]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[111]
MQTT	Scenario	Infrastructure		RTE		TB	2021-05	[111]
Nessus	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-05	[111]
Netsniff-ng	Monitoring and Analytics	Data Collection		RTE		TB	2021-05	[111]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-05	[111]
Node-RED	Scenario	Infrastructure		RTE		TB	2021-05	[111]
Ostinato	Scenario	Traffic Generation		RTE		TB	2021-05	[111]
OWASP security Shepherd VM	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[111]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2021-05	[111]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-05	[111]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Vmware NSX	Network Infrastructure	Network Virtualization		RTE		TB	2021-05	[111]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2021-05	[111]
Zeek	Custom Development	Dataset Generation		RTE		TB	2021-05	[111]
DNP3	Scenario	Infrastructure		RTE		TB	2024-01	[122]
EXata network modelling	Network Infrastructure	Network Virtualization		RTE		TB	2024-01	[122]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-01	[122]
RSCAD simulation software	Scenario	Create/Edit		RTE		TB	2024-01	[122]
RTDS simulator	Scenario	Simulation and Emulation		RTE		TB	2024-01	[122]
DNP3	Scenario	Infrastructure		RTE		TB	2024-09	[123]
EXata CPS (Cyber-Physical Network Simulator)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-09	[123]
IEC61850	Scenario	Infrastructure		RTE		TB	2024-09	[123]
IEEE C37.118	Scenario	Infrastructure		RTE		TB	2024-09	[123]
Modbus	Scenario	Create/Edit		RTE		TB	2024-09	[123]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-09	[123]
RTDS simulator	Scenario	Simulation and Emulation		RTE		TB	2024-09	[123]
RT-LAB	Scenario	Simulation and Emulation		RTE		TB	2024-09	[123]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[123]
DNP3	Scenario	Infrastructure		RTE		TB	2021-07	[36]
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2021-07	[36]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2021-07	[36]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2021-07	[36]
Modbus	Scenario	Infrastructure		RTE		TB	2021-07	[36]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2021-07	[36]
Shodan	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-07	[36]
HYPERSIM	Scenario	Simulation and Emulation		RTE		TB	2025-03	[146]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MongoDB	Data Storage	NoSQL Database		RTE		TB	2025-03	[146]
OCPP	Scenario	Infrastructure		RTE		TB	2025-03	[146]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2025-03	[146]
SQLite	Data Storage	Relational Database		RTE		TB	2025-03	[146]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-03	[146]
Controller Area Network (CAN)	Scenario	Infrastructure		RTE		TB	2022-10	[9]
Avet	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-05	[187]
DVWA	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[187]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-05	[187]
Owasp Zap (Zed Attack Proxy)	Red Team Operations	Proxy and Web Interception		RTE		TB	2021-05	[187]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2025-07	[75]
Chanalyzer	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-07	[75]
dsniff	Red Team Operations	Paketmanipulation		RTE		TB	2025-07	[75]
LoRaWAN	Scenario	Infrastructure		RTE		TB	2025-07	[75]
Mirai	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-07	[75]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2025-07	[75]
WirelessHART	Scenario	Infrastructure		RTE		TB	2025-07	[75]
GAMS	Scenario	Create/Edit		RTE		TB	2021-12	[46]
GOOSE	Scenario	Infrastructure		RTE		TB	2021-12	[46]
IEC 60870-5-104	Scenario	Infrastructure		RTE		TB	2021-12	[46]
MATLAB/Simulink	Scenario	Create/Edit		RTE		TB	2021-12	[46]
RT-LAB	Scenario	Controlling		RTE		TB	2021-12	[46]
Docker	Computing Platform	Containerisation		RTE		TB	2024-08	[185]
Grafana	Scenario	Infrastructure		RTE		TB	2024-08	[185]
MLFlow	Scenario	Infrastructure		RTE		TB	2024-08	[185]
OBS	Scenario	Infrastructure		RTE		TB	2024-08	[185]
Owncast	Scenario	Infrastructure		RTE		TB	2024-08	[185]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
PostgreSQL	Data Storage	Relational Database		RTE		TB	2024-08	[185]
Pynput	Scenario	Infrastructure		RTE		TB	2024-08	[185]
DNP3	Scenario	Infrastructure		RTE	TE	TB	2024-12	[158]
Elasticsearch	Monitoring and Analytics	Log Management		RTE	TE	TB	2024-12	[158]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE	TE	TB	2024-12	[158]
Modbus	Scenario	Infrastructure		RTE	TE	TB	2024-12	[158]
NETLAB+	Portal Services	User Access		RTE	TE	TB	2024-12	[158]
OWASP Juice Shop	Red Team Operations	Training and Practice Systems		RTE	TE	TB	2024-12	[158]
PfSense	Network Infrastructure	Firewall and routing platform		RTE	TE	TB	2024-12	[158]
Security Onion	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[158]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[158]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE	TE	TB	2024-12	[158]
Windows Active Directory	Management	Identity & Access Management (IAM)		RTE	TE	TB	2024-12	[158]
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[158]
NS2	Network Infrastructure	Network Virtualization		RTE		TB	2022-09	[160]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE	TE	CR	2020-01	[91]
HashiCorp Consul	Scenario	Infrastructure		RTE	TE	CR	2020-01	[91]
OpenStack	Computing Platform	Cloud Infrastructure		RTE	TE	CR	2020-01	[91]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration		RTE	TE	CR	2020-01	[91]
Apache web server	Scenario	Infrastructure			TE	CR	2022-04	[40]
Docker	Computing Platform	Containerisation			TE	CR	2022-04	[40]
EDURange	Computing Platform	Integrated Cyber Range Solutions			TE	CR	2022-04	[40]
JSON	Scenario	Create/Edit			TE	CR	2022-04	[40]
LAMP stack	Red Team Operations	Training and Practice Systems			TE	CR	2022-04	[40]
MySQL Database	Red Team Operations	Training and Practice Systems			TE	CR	2022-04	[40]
OpenSSH	Portal Services	User Access			TE	CR	2022-04	[40]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2022-04	[40]
Virtual network computing (VNC)	Portal Services	User Access			TE	CR	2022-04	[40]
Docker	Computing Platform	Containerisation		RTE		TB	2022-05	[74]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2022-05	[74]
GOOSE	Scenario	Infrastructure		RTE		TB	2022-05	[74]
MATLAB/Simulink	Scenario	Infrastructure		RTE		TB	2022-05	[74]
MMS	Scenario	Infrastructure		RTE		TB	2022-05	[74]
MQTT	Scenario	Infrastructure		RTE		TB	2022-05	[74]
Node-RED	Scenario	Infrastructure		RTE		TB	2022-05	[74]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2022-05	[74]
SPEEDGOAT	Scenario	Simulation and Emulation		RTE		TB	2022-05	[74]
SQLite	Scenario	Create/Edit		RTE		TB	2022-05	[74]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2022-05	[74]
CARLA Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-11	[216]
KITTI Dataset	Scenario	Simulation and Emulation		RTE		TB	2024-11	[216]
GNU Radio	Scenario	Infrastructure		RTE		TB	2025-08	[129]
InfluxDB	Data Storage	Time-series database		RTE		TB	2025-08	[129]
iPerf3	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-08	[129]
Open5GS	Scenario	Infrastructure		RTE		TB	2025-08	[129]
O-RAN SC	Scenario	Infrastructure		RTE		TB	2025-08	[129]
srsRAN	Scenario	Infrastructure		RTE		TB	2025-08	[129]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2025-08	[129]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-04	[163]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-04	[163]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2022-05	[164]
Asherah NPP Simulator (ANS)	Scenario	Simulation and Emulation		RTE		TB	2024-10	[180]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-10	[180]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-10	[180]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-10	[180]
Modbus	Scenario	Infrastructure		RTE		TB	2024-10	[180]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-10	[180]
Docker	Computing Platform	Containerisation		RTE		TB	2025-06	[101]
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2025-06	[101]

Table 14 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2025-06	[101]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2025-06	[101]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-06	[101]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2025-06	[101]
Modbus	Scenario	Infrastructure		RTE		TB	2025-06	[101]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-06	[101]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-06	[101]
Proxmox VE	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-06	[101]
SCADA-LTS	Scenario	Simulation and Emulation		RTE		TB	2025-06	[101]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2025-06	[101]
Sguil	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-06	[101]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-06	[101]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-06	[101]
Apache Parquet	Custom Development	Dataset Generation		RTE		TB	2025-06	[79]
Arpspoof	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-06	[79]
Modbus	Scenario	Infrastructure		RTE		TB	2025-06	[79]
NSRDB (National Solar Radiation Database)	Scenario	Simulation and Emulation		RTE		TB	2025-06	[79]
Pandapower	Scenario	Simulation and Emulation		RTE		TB	2025-06	[79]
pvlib	Scenario	Simulation and Emulation		RTE		TB	2025-06	[79]
rsyslog	Monitoring and Analytics	Log Management		RTE		TB	2025-06	[79]
S7comm	Scenario	Infrastructure		RTE		TB	2025-06	[79]
scapy	Red Team Operations	Paketmanipulation		RTE		TB	2025-06	[79]

Table 15 Data repository (Part 2/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Siemens windows control centre (WinCC)	Scenario	Infrastructure	RTE			TB	2025-06	[79]
Tcpdump	Monitoring and Analytics	Data Collection	RTE			TB	2025-06	[79]
Totally Integrated Automation Portal Services (TIA Portal Services)	Scenario	Create/Edit	RTE			TB	2025-06	[79]
windpowerlib	Scenario	Simulation and Emulation	RTE			TB	2025-06	[79]
Bettercap	Red Team Operations	Exploitation and Attack Execution	RTE			TB	2025-03	[107]
Ettercap	Red Team Operations	Exploitation and Attack Execution	RTE			TB	2025-03	[107]
Metasploit	Red Team Operations	Exploitation and Attack Execution	RTE			TB	2025-03	[107]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	RTE			TB	2025-03	[107]
SSLStrip	Red Team Operations	Exploitation and Attack Execution	RTE			TB	2025-03	[107]
Tshark	Monitoring and Analytics	Analysis & Verification	RTE			TB	2025-03	[107]
Wireshark	Monitoring and Analytics	Data Collection	RTE			TB	2025-03	[107]
OpenSSH	Portal Services	Admin Access		TE		CR	2023-08	[149]
OpenStack	Computing Platform	Cloud Infrastructure		TE		CR	2023-08	[149]
proftpd	Scenario	Infrastructure		TE		CR	2023-08	[149]
TightVNC	Scenario	Infrastructure		TE		CR	2023-08	[149]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics		TE		CR	2023-08	[149]
DigitalOcean VPC	Computing Platform	Cloud Infrastructure	RTE			TB	2025-05	[12]
JSON	Blue Team Operations	SIEM & Security Analytics	RTE			TB	2025-05	[12]
LangChain	Custom Development	AI & Machine Learning	RTE			TB	2025-05	[12]
LangGraph	Custom Development	AI & Machine Learning	RTE			TB	2025-05	[12]
NATS	Scenario	Infrastructure	RTE			TB	2025-05	[12]
OpenSSH	Red Team Operations	Training and Practice Systems	RTE			TB	2025-05	[12]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	RTE			TB	2025-05	[12]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics	RTE			TB	2025-05	[12]
GRFICS	Scenario	Simulation and Emulation	RTE			TB	2025-05	[140]
GridLAB-D	Scenario	Simulation and Emulation	RTE			TB	2025-05	[140]
Mininet	Network Infrastructure	Network Virtualization	RTE			TB	2025-05	[140]
Modbus	Scenario	Create/Edit	RTE			TB	2025-05	[140]
OpenPLC	Scenario	Infrastructure	RTE			TB	2025-05	[140]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2025-05	[140]
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2022-10	[134]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure				CR	2022-06	[19]
Boto3	Computing Platform	Infrastructure Provisioning and Configuration				CR	2022-06	[19]
CyRIS	Computing Platform	Infrastructure Instantiation Systems				CR	2022-06	[19]
Bazaar Collaborative Learning Environment	Management	Learning Management System	E		TE	TB	2025-02	[124]
LAMP stack	Red Team Operations	Training and Practice Systems	E		TE	TB	2025-02	[124]
Apache Guacamole	Portal Services	Admin Access		RTE		TB	2022-05	[69]
GOOSE	Scenario	Infrastructure		RTE		TB	2022-05	[69]
OPNSense	Network Infrastructure	Firewall and routing platform		RTE		TB	2022-05	[69]
VMWare ESXi	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2022-05	[69]
Apache ARIA	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2020-08	[150]
Apache web server	Red Team Operations	Training and Practice Systems			TE	CR	2020-08	[150]
DevStack	Computing Platform	Cloud Infrastructure			TE	CR	2020-08	[150]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting			TE	CR	2020-08	[150]
Nmap	Red Team Operations	Network Scanning and Reconnaissance			TE	CR	2020-08	[150]
OpenStack	Computing Platform	Cloud Infrastructure			TE	CR	2020-08	[150]
PyDatalog	Red Team Operations	Attack Strategy & Support			TE	CR	2020-08	[150]
rockyou wordlist	Red Team Operations	Attack Strategy & Support			TE	CR	2020-08	[150]
Wordpress	Red Team Operations	Training and Practice Systems			TE	CR	2020-08	[150]
YAML	Scenario	Create/Edit			TE	CR	2020-08	[150]
Java Spring	Custom Development	Backend Frameworks		RTE		TB	2025-08	[39]
Kubernetes	Computing Platform	Container Orchestration		RTE		TB	2025-08	[39]
Locust	Scenario	Traffic Generation		RTE		TB	2025-08	[39]
MongoDB	Data Storage	NoSQL Database		RTE		TB	2025-08	[39]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2025-08	[39]
tcconfig	Scenario	Infrastructure		RTE		TB	2025-08	[39]
CyTrONE	Computing Platform	Integrated Cyber Range Solutions				CR	2023-01	[17]
KYPO	Computing Platform	Integrated Cyber Range Solutions				CR	2023-01	[17]
MBRL-Lib (Meta)	Scenario	Infrastructure		RTE		TB	2024-09	[135]
Microsoft DoWhy	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[135]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[135]
Scikit-learn	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[135]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[135]
YAWNING-TITAN (YT)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-09	[135]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
COPA Zenon SCADA	Scenario	Infrastructure				TB	2021-12	[127]
Dragos OT Asset Visibility and Inventory	Management	Asset & Infrastructure Management				TB	2021-12	[127]
ELK Stack	Monitoring and Analytics	Log Management				TB	2021-12	[127]
GOOSE	Scenario	Infrastructure				TB	2021-12	[127]
Kibana	Monitoring and Analytics	Visualization & Dashboarding				TB	2021-12	[127]
Microsoft Sysmon	Monitoring and Analytics	Log Management				TB	2021-12	[127]
MMS	Scenario	Infrastructure				TB	2021-12	[127]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				TB	2021-12	[127]
Wazuh HIDS	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				TB	2021-12	[127]
Windows Active Directory	Portal Services	Identity & Access Management (IAM)				TB	2021-12	[127]
CICIOT-2023	Scenario	Infrastructure		RTE		TB	2025-01	[53]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-01	[53]
NumPy	Custom Development	Data Science		RTE		TB	2025-01	[53]
OpenDaylight	Scenario	Infrastructure		RTE		TB	2025-01	[53]
P4 BMv2 software switch	Scenario	Infrastructure		RTE		TB	2025-01	[53]
Pandas	Custom Development	Data Science		RTE		TB	2025-01	[53]
Scikit-learn	Custom Development	AI & Machine Learning		RTE		TB	2025-01	[53]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-01	[53]
Xterm	Scenario	Traffic Generation		RTE		TB	2025-01	[53]
Docker	Computing Platform	Containerisation		RTE		TB	2024-10	[102]
Ettercap	Red Team Operations	Proxy and Web Interception		RTE		TB	2024-10	[102]
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2024-10	[102]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-10	[102]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-10	[102]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2024-10	[102]
Modbus	Scenario	Infrastructure		RTE		TB	2024-10	[102]
OpenFlow	Scenario	Infrastructure		RTE		TB	2024-10	[102]
OpenPLC	Management	Platform & Environment Management		RTE		TB	2024-10	[102]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2024-10	[102]
pigrelay	Blue Team Operations	Endpoint Detection & Response (EDR)		RTE		TB	2024-10	[102]
Ryu	Scenario	Infrastructure		RTE		TB	2024-10	[102]
SCADA-LTS	Scenario	Simulation and Emulation		RTE		TB	2024-10	[102]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-10	[102]
CORE	Network Infrastructure	Network Virtualization		RTE		TB	2021-08	[178]
Minimega	Computing Platform	Integrated Cyber Range Solutions		RTE		TB	2021-08	[178]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-08	[178]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2021-08	[178]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2021-08	[178]
Docker	Computing Platform	Containerisation	E		TE	CR	2024-09	[60]
Ettercap	Red Team Operations	Paketmanipulation	E		TE	CR	2024-09	[60]
Flask	Custom Development	Backend Frameworks	E		TE	CR	2024-09	[60]
Google Firebase	Management	User Management	E		TE	CR	2024-09	[60]
Mininet	Network Infrastructure	Network Virtualization	E		TE	CR	2024-09	[60]
VueJS	Custom Development	Frontend Frameworks	E		TE	CR	2024-09	[60]
CSV	Monitoring and Analytics	Log Management	E	RTE		TB	2025-03	[174]
Elastic Filebeat	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[174]
Elastic Logstash	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[174]
Elasticsearch	Data Storage	Event and Log Storage		RTE		TB	2025-03	[174]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-03	[174]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2025-03	[174]
MITRE Caldera	Red Team Operations	Adversary emulation		RTE		TB	2025-03	[174]
Winlogbeat	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[174]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-04	[196]
Factory I/O	Scenario	Simulation and Emulation		RTE		TB	2025-04	[196]
Modbus	Scenario	Create/Edit		RTE		TB	2025-04	[196]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-04	[196]
PfSense	Network Infrastructure	Firewall and routing platform		RTE		TB	2025-04	[196]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[196]
UM-NIDS	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[196]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[196]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE		CR	2024-10	[35]
Docker	Computing Platform	Containerisation		RTE		CR	2024-10	[35]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Docker Swarm	Computing Platform	Container Orchestration		RTE		CR	2024-10	[35]
Flask	Custom Development	Backend Frameworks		RTE		CR	2024-10	[35]
JSON	Computing Platform	Infrastructure Provisioning and Configuration		RTE		CR	2024-10	[35]
libIEC61850	Scenario	Infrastructure		RTE		CR	2024-10	[35]
MySQL Database	Red Team Operations	Training and Practice Systems		RTE		CR	2024-10	[35]
OpenJDK 8	Custom Development	Runtime Environment		RTE		CR	2024-10	[35]
OpenPLC	Scenario	Infrastructure		RTE		CR	2024-10	[35]
OpenSSH	Portal Services	User Access		RTE		CR	2024-10	[35]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		CR	2024-10	[35]
Pandapower	Scenario	Simulation and Emulation		RTE		CR	2024-10	[35]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		CR	2024-10	[35]
scapy	Red Team Operations	Paketmanipulation		RTE		CR	2024-10	[35]
Virtual network computing (VNC)	Portal Services	User Access		RTE		CR	2024-10	[35]
Wireshark	Monitoring and Analytics	Data Collection		RTE		CR	2024-10	[35]
Apache Bench	Scenario	Traffic Generation		RTE		TB	2025-08	[130]
Apache web server	Scenario	Infrastructure		RTE		TB	2025-08	[130]
bpftrace	Scenario	Create/Edit		RTE		TB	2025-08	[130]
eBPF	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-08	[130]
Kubernetes	Computing Platform	Container Orchestration		RTE		TB	2025-08	[130]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-08	[130]
libbpf	Scenario	Create/Edit		RTE		TB	2025-08	[130]
Libvirt	Computing Platform	Infrastructure Provisioning and Configuration		RTE		TB	2025-08	[130]
MySQL Database	Data Storage	Relational Database		RTE		TB	2025-08	[130]
Nginx Web server	Scenario	Infrastructure		RTE		TB	2025-08	[130]
Redis database	Data Storage	NoSQL Database		RTE		TB	2025-08	[130]
sysbench	Scenario	Traffic Generation		RTE		TB	2025-08	[130]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-08	[130]
Tomcat web server	Scenario	Infrastructure		RTE		TB	2025-08	[130]
Afra	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-06	[110]
Lingua Franca	Scenario	Create/Edit		RTE		TB	2024-06	[110]
ltsconvert	Scenario	Infrastructure		RTE		TB	2024-06	[110]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Timed Rebeca	Scenario	Simulation and Emulation		RTE		TB	2024-06	[110]
Apache Guacamole	Portal Services	User Access	E			CR	2023-03	[68]
Docker	Computing Platform	Containerisation	E			CR	2023-03	[68]
Google Cloud	Computing Platform	Cloud Infrastructure	E			CR	2023-03	[68]
NoSQL database	Data Storage	NoSQL Database	E			CR	2023-03	[68]
Virtual network computing (VNC)	Portal Services	User Access	E			CR	2023-03	[68]
Windows Remote desktop protocol (RDP)	Portal Services	User Access	E			CR	2023-03	[68]
YAML	Scenario	Create/Edit	E			CR	2023-03	[68]
CTFd	Red Team Operations	Training and Practice Systems	E		TE	CR	2023-12	[151]
OPNSense	Network Infrastructure	Firewall and routing platform	E		TE	CR	2023-12	[151]
bwm-ng	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2021-06	[193]
Coin Hive	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[193]
Docker	Computing Platform	Containerisation	E		TE	CR	2021-06	[193]
GENI cloud	Computing Platform	Cloud Infrastructure	E		TE	CR	2021-06	[193]
Geth	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[193]
MariaDB	Data Storage	Relational Database	E		TE	CR	2021-06	[193]
Slowhttptest	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[193]
Spring Boot	Custom Development	Backend Frameworks	E		TE	CR	2021-06	[193]
Wireshark	Monitoring and Analytics	Data Collection	E		TE	CR	2021-06	[193]
Ansible	Computing Platform	Software Provisioning and Configuration				CR	2023-12	[126]
Microsoft SQL Database	Data Storage	Relational Database				CR	2023-12	[126]
MySQL Database	Data Storage	Relational Database				CR	2023-12	[126]
SharePoint	Management	Content and Document Management				CR	2023-12	[126]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration				CR	2023-12	[126]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor				CR	2023-12	[126]
Windows Active Directory	Management	Identity & Access Management (IAM)				CR	2023-12	[126]
Jupyter notebook	Custom Development	Integrated Development Environment		RTE		TB	2023-11	[20]
Matplotlib	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2023-11	[20]
NumPy	Custom Development	Data Science		RTE		TB	2023-11	[20]
Pandas	Custom Development	Data Science		RTE		TB	2023-11	[20]

Table 15 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
CURA	Red Team Operations	Training and Practice Systems		RTE		TB	2020-01	[169]
MySQL Database	Data Storage	Relational Database		RTE		TB	2020-01	[169]
OpenPLC	Scenario	Infrastructure		RTE		TB	2020-01	[169]
scapy	Management	Platform & Environment Management		RTE		TB	2020-01	[169]
Docker	Computing Platform	Containerisation		RTE		TB	2025-05	[90]
jMAVSim	Scenario	Simulation and Emulation		RTE		TB	2025-05	[90]
MAVLink	Scenario	Infrastructure		RTE		TB	2025-05	[90]
MySQL Database	Data Storage	Relational Database		RTE		TB	2025-05	[90]
PX4 Autopilot	Scenario	Simulation and Emulation		RTE		TB	2025-05	[90]
pymavlink	Monitoring and Analytics	Data Collection		RTE		TB	2025-05	[90]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2020-04	[157]
OpenDSS	Network Infrastructure	Network Virtualization		RTE		TB	2020-04	[157]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[139]
MQTT	Scenario	Infrastructure		RTE		TB	2025-03	[139]
OpenDSS	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[139]
Typhoon-HIL	Scenario	Simulation and Emulation		RTE		TB	2025-03	[139]
Cydarm	Management	Workflow & Orchestration		RTE		CR	2025-05	[81]
GPT-4o	Blue Team Operations	SIEM & Security Analytics		RTE		CR	2025-05	[81]
LlamaIndex	Custom Development	AI & Machine Learning		RTE		CR	2025-05	[81]
MITRE ATT&CK	Blue Team Operations	Threat Intelligence		RTE		CR	2025-05	[81]
Slack	Monitoring and Analytics	Visualization & Dashboarding		RTE		CR	2025-05	[81]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics		RTE		CR	2025-05	[81]
Apache Guacamole	Portal Services	User Access	E			CR	2023-10	[66]
Authentik	Portal Services	Identity & Access Management (IAM)	E			CR	2023-10	[66]
CSV	Management	User Management	E			CR	2023-10	[66]
DUO 2FA	Portal Services	Identity & Access Management (IAM)	E			CR	2023-10	[66]
Elasticsearch	Monitoring and Analytics	Log Management	E			CR	2023-10	[66]
Foreman	Computing Platform	Infrastructure Provisioning and Configuration	E			CR	2023-10	[66]
Kubevirt	Computing Platform	Infrastructure Provisioning and Configuration	E			CR	2023-10	[66]
Libvirt	Computing Platform	Infrastructure Provisioning and Configuration	E			CR	2023-10	[66]
Nginx Proxy Manager	Network Infrastructure	Reverse-Proxy	E			CR	2023-10	[66]
OpenLDAP	Management	User Management	E			CR	2023-10	[66]
PfSense	Network Infrastructure	Firewall and routing platform	E			CR	2023-10	[66]

Table 16 Data repository (Part 3/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Proxmox VE	Computing Platform	Virtualization platform/Type-1-Hypervisor	E			CR	2023-10	[66]
LAMP stack	Management	Platform & Environment Management				CR	2021-12	[162]
OpenStack	Computing Platform	Cloud Infrastructure				CR	2021-12	[162]
CarSim	Scenario	Simulation and Emulation		RTE		TB	2024-12	[147]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-12	[147]
Asherah NPP Simulator (ANS)	Scenario	Simulation and Emulation		RTE		TB	2021-09	[28]
IPFire	Network Infrastructure	Firewall and routing platform		RTE		TB	2021-09	[28]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2021-09	[28]
Modbus	Scenario	Infrastructure		RTE		TB	2021-09	[28]
OPC Data Access	Scenario	Infrastructure		RTE		TB	2021-09	[28]
OPC Unified Architecture (OPC-UA)	Scenario	Infrastructure		RTE		TB	2021-09	[28]
PARCS	Management	Platform & Environment Management		RTE		TB	2021-09	[28]
R5	Management	Platform & Environment Management		RTE		TB	2021-09	[28]
ScadaBR	Scenario	Simulation and Emulation		RTE		TB	2021-09	[28]
Clonezilla	Computing Platform	Infrastructure Provisioning and Configuration		RTE		CR	2021-07	[117]
DEEP EXPLOIT	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2021-07	[117]
Docker	Computing Platform	Containerisation		RTE		CR	2021-07	[117]
InsightVM	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2021-07	[117]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		CR	2021-07	[117]
Nikto	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
Nmap	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
OpenVAS	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
Owasp Zap (Zed Attack Proxy)	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
OwaspBWA	Red Team Operations	Training and Practice Systems		RTE		CR	2021-07	[117]
SecGen	Scenario	Create/Edit		RTE		CR	2021-07	[117]
SkipFish	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[117]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		CR	2021-07	[117]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2021-07	[117]
Datasets	Custom Development	AI & Machine Learning		RTE		CR	2023-03	[51]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Keras	Custom Development	Data Science		RTE		CR	2023-03	[51]
Pandas	Custom Development	Data Science		RTE		CR	2023-03	[51]
PrettyTable	Custom Development	Visualization & Dashboarding		RTE		CR	2023-03	[51]
Scikit-learn	Custom Development	AI & Machine Learning		RTE		CR	2023-03	[51]
Scipy	Custom Development	Data Science		RTE		CR	2023-03	[51]
Setuptools	Custom Development	Build-Toolchain		RTE		CR	2023-03	[51]
TensorFlow	Custom Development	AI & Machine Learning		RTE		CR	2023-03	[51]
Transformers	Custom Development	AI & Machine Learning		RTE		CR	2023-03	[51]
AMQP	Scenario	Infrastructure		RTE		TB	2025-06	[54]
Apache Flume	Monitoring and Analytics	Data Collection		RTE		TB	2025-06	[54]
Apache Kafka	Monitoring and Analytics	Data Collection		RTE		TB	2025-06	[54]
CICIOT-2023	Scenario	Infrastructure		RTE		TB	2025-06	[54]
Microsoft Azure	Computing Platform	Cloud Infrastructure		RTE		TB	2025-06	[54]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-06	[54]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-06	[54]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-06	[54]
Apache SkyWalking	Scenario	Create/Edit		RTE		TB	2025-02	[177]
DeepLog	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[177]
EFK-Stack	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[177]
Free5GC	Scenario	Infrastructure		RTE		TB	2025-02	[177]
h2load	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-02	[177]
Helm	Computing Platform	Container Orchestration		RTE		TB	2025-02	[177]
Istio	Scenario	Create/Edit		RTE		TB	2025-02	[177]
Kubernetes	Computing Platform	Container Orchestration		RTE		TB	2025-02	[177]
LogAnomaly	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[177]
UERANSIM	Scenario	Infrastructure		RTE		TB	2025-02	[177]
Docker	Computing Platform	Containerisation	E	RTE	TE	CR	2021-06	[104]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Elastic Beats	Monitoring and Analytics	Log Management	E	RTE	TE	CR	2021-06	[104]
Elastic Logstash	Monitoring and Analytics	Log Management	E	RTE	TE	CR	2021-06	[104]
Elasticsearch	Monitoring and Analytics	Log Management	E	RTE	TE	CR	2021-06	[104]
Kibana	Monitoring and Analytics	Visualization & Dashboarding	E	RTE	TE	CR	2021-06	[104]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization	E	RTE	TE	CR	2021-06	[104]
Syslog	Monitoring and Analytics	Log Management	E	RTE	TE	CR	2021-06	[104]
TheHive	Blue Team Operations	Incident Management & Response	E	RTE	TE	CR	2021-06	[104]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor	E	RTE	TE	CR	2021-06	[104]
Wireguard	Portal Services	User Access	E	RTE	TE	CR	2021-06	[104]
MQTT	Scenario	Infrastructure			TE	TB	2023-10	[32]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE	TE	CR	2024-05	[21]
AWX	Computing Platform	Software Provisioning and Configuration		RTE	TE	CR	2024-05	[21]
Harvester	Computing Platform	Infrastructure Provisioning and Configuration		RTE	TE	CR	2024-05	[21]
Kubernetes	Computing Platform	Container Orchestration		RTE	TE	CR	2024-05	[21]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	CR	2024-05	[21]
Node-RED	Red Team Operations	Attack Strategy & Support		RTE	TE	CR	2024-05	[21]
Rancher	Computing Platform	Container Orchestration		RTE	TE	CR	2024-05	[21]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE	TE	CR	2024-05	[21]
DVWA	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[138]
EVE community edition	Network Infrastructure	Network Virtualization		RTE	TE	CR	2023-04	[138]
Fortinet's log (15-day trial):	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[138]
Fortinet's WAF (15-day trial):	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[138]
Huawei's firewall (30-day trial)	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[138]
VMWare	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE	TE	CR	2023-04	[138]
Bettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2020-01	[2]
Binwalk	Red Team Operations	Reverse Engineering and Binary Analysis		RTE		TB	2020-01	[2]
Dex2jar	Red Team Operations	Reverse Engineering and Binary Analysis		RTE		TB	2020-01	[2]
Dirb	Red Team Operations	Brute force attacks		RTE		TB	2020-01	[2]
DirBuster	Red Team Operations	Brute force attacks		RTE		TB	2020-01	[2]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2020-01	[2]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2020-01	[2]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2020-01	[2]
Owasp Zap (Zed Attack Proxy)	Red Team Operations	Vulnerability Management		RTE		TB	2020-01	[2]
Shodan	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2020-01	[2]
SkipFish	Red Team Operations	Vulnerability Management		RTE		TB	2020-01	[2]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2020-01	[2]
SSLStrip	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2020-01	[2]
Tshark	Blue Team Operations	Network Analysis & Reconnaissance		RTE		TB	2020-01	[2]
WAFWoof	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2020-01	[2]
Wascan	Red Team Operations	Vulnerability Management		RTE		TB	2020-01	[2]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2020-01	[2]
LAMP stack	Red Team Operations	Training and Practice Systems			TE	CR	2022-10	[100]
Metasploit	Red Team Operations	Exploitation and Attack Execution			TE	CR	2022-10	[100]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor			TE	CR	2022-10	[100]
WAMP stack	Red Team Operations	Training and Practice Systems			TE	CR	2022-10	[100]
DIATEAMs Hybrid Network Simulation (HNS) cyber range platform	Computing Platform	Integrated Cyber Range Solutions				CR	2022-07	[11]
Maritime Cyber Risk Analysis (MaCRA)	Monitoring and Analytics	Analysis & Verification				CR	2022-07	[11]
RabbitMQ	Scenario	Infrastructure				CR	2022-07	[11]
CollectD	Monitoring and Analytics	Analysis & Verification		RTE		TB	2022-12	[41]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2022-12	[41]
Hydra	Red Team Operations	Brute force attacks		RTE		TB	2022-12	[41]
InfluxDB	Data Storage	Time-series database		RTE		TB	2022-12	[41]
LabView	Monitoring and Analytics	Data Collection		RTE		TB	2022-12	[41]
MQTT	Scenario	Infrastructure		RTE		TB	2022-12	[41]
NXPs FreeMASTER Run Time Debugging Tool	Scenario	Infrastructure		RTE		TB	2022-12	[41]
S32 Design Studio IDE	Scenario	Infrastructure		RTE		TB	2022-12	[41]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Tshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2022-12	[41]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2022-12	[41]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-05	[8]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-05	[8]
OpenDaylight	Scenario	Infrastructure		RTE		TB	2025-05	[8]
OpenFlow	Scenario	Infrastructure		RTE		TB	2025-05	[8]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2025-05	[8]
sFlow	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-05	[8]
sFlow-RT	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-05	[8]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-05	[8]
Amazon API Gateway	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon AppSync	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon CloudWatch	Monitoring and Analytics	Log Management		RTE		TB	2024-12	[14]
Amazon DynamoDB	Data Storage	NoSQL Database		RTE		TB	2024-12	[14]
Amazon EventBridge	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon Route 53	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon SES	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon SNS	Scenario	Infrastructure		RTE		TB	2024-12	[14]
Amazon SQS	Scenario	Infrastructure		RTE		TB	2024-12	[14]
AWS CloudTrail	Monitoring and Analytics	Log Management		RTE		TB	2024-12	[14]
AWS Elemental MediaConvert	Scenario	Infrastructure		RTE		TB	2024-12	[14]
AWS Lambda	Scenario	Infrastructure		RTE		TB	2024-12	[14]
AWS S3	Data Storage	Object Storage		RTE		TB	2024-12	[14]
AWS Step Functions	Scenario	Infrastructure		RTE		TB	2024-12	[14]
AWS X-Ray	Monitoring and Analytics	Log Management		RTE		TB	2024-12	[14]
Boto3	Scenario	Infrastructure		RTE		TB	2024-12	[14]
chars2vec	Scenario	Infrastructure		RTE		TB	2024-12	[14]
ARTEMIS real-time simulator	Scenario	Simulation and Emulation		RTE		TB	2023-12	[114]
eMEGASIM	Scenario	Simulation and Emulation		RTE		TB	2023-12	[114]
EXata network modelling	Network Infrastructure	Network Virtualization		RTE		TB	2023-12	[114]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2023-12	[114]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2023-12	[114]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Python Flask framework	Custom Development	Backend Frameworks		RTE		TB	2023-12	[114]
React.js	Custom Development	Frontend Frameworks		RTE		TB	2023-12	[114]
Factory I/O	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[154]
MATLAB/Simulink	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[154]
Modbus	Scenario	Infrastructure	E		TE	CR	2023-06	[154]
Node-RED	Scenario	Infrastructure	E		TE	CR	2023-06	[154]
OpenPLC	Scenario	Infrastructure	E		TE	CR	2023-06	[154]
PfSense	Network Infrastructure	Firewall and routing platform	E		TE	CR	2023-06	[154]
ScadaBR	Red Team Operations	Training and Practice Systems	E		TE	CR	2023-06	[154]
Unity3D	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[154]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor	E		TE	CR	2023-06	[154]
Modbus	Scenario	Create/Edit		RTE		TB	2024-10	[170]
NS3	Network Infrastructure	Network Virtualization		RTE		TB	2024-10	[170]
RTDS	Scenario	Simulation and Emulation		RTE		TB	2024-10	[170]
LightGBM	Custom Development	AI & Machine Learning		RTE		CR	2022-08	[217]
Modbus	Scenario	Infrastructure		RTE		CR	2022-08	[217]
OPC Unified Architecture (OPC-UA)	Scenario	Infrastructure		RTE		CR	2022-08	[217]
Unity3D	Scenario	Simulation and Emulation		RTE		CR	2022-08	[217]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-08	[98]
Factory I/O	Scenario	Simulation and Emulation		RTE		TB	2024-08	[98]
Google Colab	Custom Development	AI & Machine Learning		RTE		TB	2024-08	[98]
OpenPLC	Scenario	Infrastructure		RTE		TB	2024-08	[98]
sktime	Custom Development	AI & Machine Learning		RTE		TB	2024-08	[98]
Android Emulator	Scenario	Simulation and Emulation		RTE	TE	CR	2022-07	[30]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Docker	Computing Platform	Containerisation		RTE	TE	CR	2022-07	[30]
Ghidra	Red Team Operations	Reverse Engineering and Binary Analysis		RTE	TE	CR	2022-07	[30]
Gophish	Red Team Operations	Phishing and Social Engineering		RTE	TE	CR	2022-07	[30]
iOS Simulator	Scenario	Simulation and Emulation		RTE	TE	CR	2022-07	[30]
Nginx Web server	Scenario	Infrastructure		RTE	TE	CR	2022-07	[30]
Node.js	Custom Development	Backend Frameworks		RTE	TE	CR	2022-07	[30]
React.js	Custom Development	Frontend Frameworks		RTE	TE	CR	2022-07	[30]
srcpy	Portal Services	User Access		RTE	TE	CR	2022-07	[30]
websockify	Portal Services	User Access		RTE	TE	CR	2022-07	[30]
Wi-Fi Baby Monitor	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2022-07	[30]
x11vnc	Portal Services	User Access		RTE	TE	CR	2022-07	[30]
9p	Management	Platform & Environment Management	E		TE	CR	2024-03	[120]
Docker	Computing Platform	Containerisation	E		TE	CR	2024-03	[120]
Gdb	Custom Development	Debugger	E		TE	CR	2024-03	[120]
Gef	Custom Development	Debugger	E		TE	CR	2024-03	[120]
Ghidra	Blue Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2024-03	[120]
Ipython	Custom Development	Integrated Development Environment	E		TE	CR	2024-03	[120]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	E		TE	CR	2024-03	[120]
OpenSSH	Portal Services	User Access	E		TE	CR	2024-03	[120]
Pwndbg	Red Team Operations	Attack Strategy & Support	E		TE	CR	2024-03	[120]
Pwntools	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2024-03	[120]
QEMU	Computing Platform	Virtualization platform/Type-2-Hypervisor	E		TE	CR	2024-03	[120]
Radare2	Blue Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2024-03	[120]

Table 16 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
scapy	Red Team Operations	Paketmanipulation	E		TE	CR	2024-03	[120]
SLIRP	Scenario	Infrastructure	E		TE	CR	2024-03	[120]
Strace	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2024-03	[120]
Tmux	Portal Services	User Access	E		TE	CR	2024-03	[120]
VS Code	Portal Services	User Access	E		TE	CR	2024-03	[120]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E		TE	CR	2024-03	[120]
HYPERSIM	Scenario	Simulation and Emulation		RTE		TB	2024-01	[155]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-01	[155]
OpalTarget OP5707XG	Scenario	Simulation and Emulation		RTE		TB	2024-01	[155]
Open Charge Point Protocol (OCPP)	Scenario	Infrastructure		RTE		TB	2024-01	[155]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-01	[155]
aircrack-ng	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[133]
Airgeddon	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[133]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2024-12	[133]
Arduino IDE	Custom Development	Integrated Development Environment		RTE		TB	2024-12	[133]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-12	[133]
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2024-12	[133]
Flower Framework	Custom Development	AI & Machine Learning		RTE		TB	2024-12	[133]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2024-12	[133]
Hping	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[133]
MySQL Database	Data Storage	Relational Database		RTE		TB	2024-12	[133]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[133]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[133]
Tracemalloc	Scenario	Infrastructure		RTE		TB	2024-12	[133]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[133]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[133]
DNP3	Scenario	Infrastructure			TE	TB	2020-10	[143]
GOOSE	Scenario	Infrastructure			TE	TB	2020-10	[143]

Table 17 Data repository (Part 4/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MMS	Scenario	Infrastructure			TE	TB	2020-10	[143]
Opal-RT Simulator	Scenario	Simulation and Emulation			TE	TB	2020-10	[143]
OpenPDC	Scenario	Simulation and Emulation			TE	TB	2020-10	[143]
RT-LAB	Scenario	Simulation and Emulation			TE	TB	2020-10	[143]
SIEMENS SICAM PAS	Scenario	Infrastructure			TE	TB	2020-10	[143]
VMWare	Computing Platform	Virtualization platform/Type-2-Hypervisor			TE	TB	2020-10	[143]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-12	[182]
Memtester	Scenario	Infrastructure		RTE		TB	2024-12	[182]
Mosquitto MQTT Broker	Red Team Operations	Training and Practice Systems		RTE		TB	2024-12	[182]
MQTT benchmarking tool	Scenario	Infrastructure		RTE		TB	2024-12	[182]
5g-trace-visualizer	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[200]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-09	[200]
Free5GC	Scenario	Infrastructure		RTE		TB	2024-09	[200]
free5gc-compose	Scenario	Create/Edit		RTE		TB	2024-09	[200]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2024-09	[200]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[200]
Transformers	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[200]
Tshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[200]
UERANSIM	Scenario	Infrastructure		RTE		TB	2024-09	[200]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[200]
Cyber Kill Chain (CKC)	Red Team Operations	Attack Strategy & Support		RTE		TB	2024-09	[13]
IEC 60870-5-104	Scenario	Infrastructure		RTE		TB	2024-09	[13]
IEC61850	Scenario	Infrastructure		RTE		TB	2024-09	[13]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-09	[13]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2024-09	[13]
MITRE Caldera	Red Team Operations	Adversary emulation		RTE		TB	2024-09	[13]
Modbus	Scenario	Infrastructure		RTE		TB	2024-09	[13]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-09	[13]
STRIDE (Microsoft)	Red Team Operations	Attack Strategy & Support		RTE		TB	2024-09	[13]
CSV	Custom Development	Dataset Generation		RTE		TB	2025-04	[77]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
curl-loader	Scenario	Traffic Generation		RTE		TB	2025-04	[77]
D-ITG	Scenario	Traffic Generation		RTE		TB	2025-04	[77]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-04	[77]
httperf	Scenario	Traffic Generation		RTE		TB	2025-04	[77]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		TB	2025-04	[77]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-04	[77]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2025-04	[77]
Ryu	Scenario	Infrastructure		RTE		TB	2025-04	[77]
Slowhttptest	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-04	[77]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-04	[77]
Libvirt	Computing Platform	Infrastructure Provisioning and Configuration		RTE		TB	2024-06	[56]
OpenDaylight	Scenario	Infrastructure		RTE		TB	2024-06	[56]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2024-06	[56]
QEMU	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-06	[56]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-06	[56]
Apache web server	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[192]
CTFd	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[192]
Docker	Computing Platform	Containerisation	E		TE	CR	2024-05	[192]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2024-05	[192]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2024-05	[192]
MySQL Database	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[192]
Naumachia	Computing Platform	Infrastructure Instantiation Systems	E		TE	CR	2024-05	[192]
OpenSSH	Portal Services	User Access	E		TE	CR	2024-05	[192]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E		TE	CR	2024-05	[192]
Sqlmap	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2024-05	[192]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E		TE	CR	2024-05	[192]
Wordpress	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[192]
Docker	Computing Platform	Containerisation			TE	CR	2025-04	[37]
Grafana	Scenario	Infrastructure			TE	CR	2025-04	[37]
Moodle	Management	Learning Management System			TE	CR	2025-04	[37]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2025-04	[37]
Prometheus	Monitoring and Analytics	Assets Monitoring			TE	CR	2025-04	[37]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
RITA	Monitoring and Analytics	Analysis & Verification			TE	CR	2025-04	[37]
Zeek	Monitoring and Analytics	Analysis & Verification			TE	CR	2025-04	[37]
EasyBuilder	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2023-07	[55]
NetToPLCsim	Network Infrastructure	Network Virtualization		RTE		TB	2023-07	[55]
S7comm	Scenario	Create/Edit		RTE		TB	2023-07	[55]
snap7	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2023-07	[55]
Totally Integrated Automation Portal Services (TIA Portal Services)	Scenario	Create/Edit		RTE		TB	2023-07	[55]
VMWare	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2023-07	[55]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-07	[55]
GOOSE	Scenario	Infrastructure		RTE		TB	2024-08	[105]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2024-08	[105]
OpenFlow	Scenario	Infrastructure		RTE		TB	2024-08	[105]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2024-08	[105]
Ryu	Scenario	Infrastructure		RTE		TB	2024-08	[105]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-08	[105]
SV	Scenario	Infrastructure		RTE		TB	2024-08	[105]
Docker	Computing Platform	Containerisation		RTE		TB	2024-09	[183]
httperf	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[183]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-09	[183]
Memtester	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-09	[183]
simpy	Scenario	Infrastructure		RTE		TB	2024-09	[183]
TeaStore	Red Team Operations	Training and Practice Systems		RTE		TB	2024-09	[183]
TimeNET	Scenario	Infrastructure		RTE		TB	2024-09	[183]
Ansible	Computing Platform	Software Provisioning and Configuration	E		TE	CR	2024-07	[89]
Elasticsearch	Monitoring and Analytics	Log Management	E		TE	CR	2024-07	[89]
Grafana	Monitoring and Analytics	Visualization & Dashboarding	E		TE	CR	2024-07	[89]
JSON	Scenario	Infrastructure	E		TE	CR	2024-07	[89]
Kibana	Monitoring and Analytics	Visualization & Dashboarding	E		TE	CR	2024-07	[89]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2024-07	[89]
Prometheus	Monitoring and Analytics	Assets Monitoring	E		TE	CR	2024-07	[89]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
airmon-ng	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[115]
EXata CPS (Cyber-Physical Network Simulator)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-04	[115]
hcitool scan	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[115]
Medusa	Red Team Operations	Brute force attacks		RTE		TB	2024-04	[115]
MobSF (Mobile Security Framework)	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2024-04	[115]
Netdiscover	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-04	[115]
Nikto	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[115]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-04	[115]
OpenVAS	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[115]
Owasp Zap (Zed Attack Proxy)	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[115]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-10	[214]
Modbus	Scenario	Infrastructure		RTE		TB	2024-10	[214]
MySQL Database	Data Storage	Relational Database		RTE		TB	2024-10	[214]
OpenWrt	Scenario	Infrastructure		RTE		TB	2024-10	[214]
pySCADA	Scenario	Simulation and Emulation		RTE		TB	2024-10	[214]
rapidSCADA	Scenario	Simulation and Emulation		RTE		TB	2024-10	[214]
rsyslog	Monitoring and Analytics	Log Management		RTE		TB	2024-10	[214]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-10	[214]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-10	[214]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-10	[214]
Gazebo	Scenario	Simulation and Emulation		RTE		TB	2025-03	[190]
MAVLink	Scenario	Infrastructure		RTE		TB	2025-03	[190]
PX4 Autopilot	Scenario	Simulation and Emulation		RTE		TB	2025-03	[190]
ROS (Robot Operating System)	Scenario	Simulation and Emulation		RTE		TB	2025-03	[190]
AERPAW (Aerial Experimentation and Research Platform for Advanced Wireless)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-01	[85]
CICIOT-2023	Scenario	Infrastructure		RTE		TB	2025-01	[85]
Flower Framework	Scenario	Controlling		RTE		TB	2025-01	[85]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
IoTBotNet-2020	Scenario	Infrastructure		RTE		TB	2025-01	[85]
iPerf3	Scenario	Traffic Generation		RTE		TB	2025-01	[85]
psutil	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-01	[85]
QGroundControl	Scenario	Infrastructure		RTE		TB	2025-01	[85]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-01	[85]
VisDrone 2021	Scenario	Infrastructure		RTE		TB	2025-01	[85]
YOLOv8	Scenario	Infrastructure		RTE		TB	2025-01	[85]
Modbus	Scenario	Infrastructure	E		TE	CR	2023-04	[87]
OpenMUC	Custom Development	Middleware	E		TE	CR	2023-04	[87]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2023-04	[87]
Ansible	Scenario	Infrastructure		RTE		TB	2023-11	[10]
Arpspoof	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2023-11	[10]
Docker	Computing Platform	Containerisation		RTE		TB	2023-11	[10]
GPRS Tunneling Protocol (GTP)	Scenario	Infrastructure		RTE		TB	2023-11	[10]
Hydra	Red Team Operations	Brute force attacks		RTE		TB	2023-11	[10]
Iptables/nftables	Red Team Operations	Attack Strategy & Support		RTE		TB	2023-11	[10]
mitmproxy	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-11	[10]
MongoDB	Data Storage	NoSQL Database		RTE		TB	2023-11	[10]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-11	[10]
Open5GS	Scenario	Infrastructure		RTE		TB	2023-11	[10]
Packet Forwarding Control Protocol (PFCP)	Scenario	Infrastructure		RTE		TB	2023-11	[10]
Tshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-11	[10]
UERANSIM	Scenario	Infrastructure		RTE		TB	2023-11	[10]
Airbus CyberRange	Computing Platform	Integrated Cyber Range Solutions		RTE		CR	2025-02	[166]
BUP Benign User Profiler	Scenario	Traffic Generation		RTE		CR	2025-02	[166]
CSV	Custom Development	Dataset Generation		RTE		CR	2025-02	[166]
HERA	Custom Development	Dataset Generation		RTE		CR	2025-02	[166]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		CR	2025-02	[166]
HULK	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		CR	2025-02	[166]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		CR	2025-02	[166]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2025-02	[166]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-02	[166]
PCAPNG	Custom Development	Dataset Generation		RTE		CR	2025-02	[166]
SecLists Password Dictionary	Red Team Operations	Attack Strategy & Support		RTE		CR	2025-02	[166]
Wireshark	Monitoring and Analytics	Data Collection		RTE		CR	2025-02	[166]
Cisco Cyber Vision	Monitoring and Analytics	Analysis & Verification			TE	TB	2021-08	[136]
Factory I/O	Scenario	Simulation and Emulation			TE	TB	2021-08	[136]
Home I/O	Scenario	Simulation and Emulation			TE	TB	2021-08	[136]
Microsoft Threat Modelling Tool	Red Team Operations	Attack Strategy & Support			TE	TB	2021-08	[136]
Modbus	Scenario	Infrastructure			TE	TB	2021-08	[136]
Nginx Web server	Red Team Operations	Attack Strategy & Support			TE	TB	2021-08	[136]
Rubber Ducky	Red Team Operations	Exploitation and Attack Execution			TE	TB	2021-08	[136]
simpy	Scenario	Infrastructure			TE	TB	2021-08	[136]
Windows Remote desktop protocol (RDP)	Red Team Operations	Attack Strategy & Support	E		TE	TB	2021-08	[136]
EXata network modelling	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[175]
HYPERSIM	Scenario	Simulation and Emulation		RTE		TB	2025-03	[175]
Modbus	Scenario	Infrastructure		RTE		TB	2025-03	[175]
CARLA	Scenario	Simulation and Emulation		RTE		TB	2025-06	[171]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2025-06	[171]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2025-06	[171]
Docker	Computing Platform	Containerisation		RTE		TB	2023-06	[47]
Ettercap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-06	[47]
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2023-06	[47]
Memcached	Scenario	Infrastructure		RTE		TB	2023-06	[47]
Modbus	Scenario	Infrastructure		RTE		TB	2023-06	[47]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-06	[47]
pyModbus	Scenario	Infrastructure		RTE		TB	2023-06	[47]
scapy	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2023-06	[47]
SQLite	Data Storage	Relational Database		RTE		TB	2023-06	[47]
Tcpdump	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-06	[47]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2023-06	[47]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2021-01	[161]
QEMU-IOL	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		CR	2021-01	[161]
Step7-MicroWin	Custom Development	Integrated Development Environment		RTE		CR	2021-01	[161]
WinSCP	Management	Platform & Environment Management		RTE		CR	2021-01	[161]
netcat	Scenario	Infrastructure		RTE		CR	2023-11	[50]
Selenium	Scenario	User Activity Simulation		RTE		CR	2023-11	[50]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		CR	2023-11	[50]
Apache Guacamole	Portal Services	User Access	E		TE	TB	2023-12	[18]
CoAP	Scenario	Infrastructure	E		TE	TB	2023-12	[18]
Contiki	Scenario	Infrastructure	E		TE	TB	2023-12	[18]
Cooja	Network Infrastructure	Network Virtualization	E		TE	TB	2023-12	[18]
Docker	Computing Platform	Containerisation	E		TE	TB	2023-12	[18]
FIT IoT-LAB	Computing Platform	Integrated Testbed Solutions	E		TE	TB	2023-12	[18]
MQTT	Scenario	Infrastructure	E		TE	TB	2023-12	[18]
RPL Protocol	Scenario	Infrastructure	E		TE	TB	2023-12	[18]
Arpspoof	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[109]
Cewl	Red Team Operations	Brute force attacks		RTE		TB	2025-03	[109]

Table 17 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[109]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[109]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2025-03	[109]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[109]
Mosquitto MQTT Broker	Red Team Operations	Training and Practice Systems		RTE		TB	2025-03	[109]
MySQL Workbench	Custom Development	Dataset Generation		RTE		TB	2025-03	[109]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[109]
Node-RED	Custom Development	Integrated Development Environment		RTE		TB	2025-03	[109]
SAir-IIoT Cyber Testbed	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-03	[109]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[109]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[109]
UFONet	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[109]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-03	[109]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-03	[109]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[109]
Xsser	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[109]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure				CR	2021-11	[179]
Packer	Computing Platform	Infrastructure Provisioning and Configuration				CR	2021-11	[179]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration				CR	2021-11	[179]
YAML	Management	Asset & Infrastructure Management				CR	2021-11	[179]
CTFd	Red Team Operations	Training and Practice Systems	E	RTE	TE	CR	2025-01	[218]
OpenStack	Computing Platform	Cloud Infrastructure	E	RTE	TE	CR	2025-01	[218]
Prometheus	Monitoring and Analytics	Assets Monitoring	E	RTE	TE	CR	2025-01	[218]

Table 18 Data repository (Part 5/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
DNP3	Scenario	Infrastructure	E		TE	CR	2020-02	[31]
Docker	Computing Platform	Containerisation	E		TE	CR	2020-02	[31]
Modbus	Scenario	Infrastructure	E		TE	CR	2020-02	[31]
MQTT	Scenario	Infrastructure	E		TE	CR	2020-02	[31]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2020-02	[31]
5Greplay	Scenario	Infrastructure		RTE		TB	2024-09	[34]
Free5GC	Scenario	Infrastructure		RTE		TB	2024-09	[34]
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2024-09	[34]
Open5GS	Scenario	Infrastructure		RTE		TB	2024-09	[34]
SCTP	Red Team Operations	Training and Practice Systems		RTE		TB	2024-09	[34]
UERANSIM	Scenario	Infrastructure		RTE		TB	2024-09	[34]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[34]
Anaconda	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
iPerf	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[78]
Jupyter notebook	Custom Development	Integrated Development Environment		RTE		TB	2024-09	[78]
Keras	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
Matplotlib	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2024-09	[78]
NumPy	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
OpenFlow	Scenario	Infrastructure		RTE		TB	2024-09	[78]
OpenvSwitch (OvS)	Network Infrastructure	Network Virtualization		RTE		TB	2024-09	[78]
Pandas	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
Pickle	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
POX	Network Infrastructure	Network Virtualization		RTE		TB	2024-09	[78]
scapy	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[78]
Scikit-learn	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
Seaborn	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
Tqdm	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[78]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-09	[78]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[78]
Asterix	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Bridge Command (BC)	Scenario	Simulation and Emulation		RTE	TE	TB	2023-07	[99]
Flatpak	Computing Platform	Infrastructure Provisioning and Configuration		RTE	TE	TB	2023-07	[99]
FUXA	Custom Development	Integrated Development Environment		RTE	TE	TB	2023-07	[99]
GNU Make	Custom Development	Build-Toolchain		RTE	TE	TB	2023-07	[99]
Modbus	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]
NATS	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]
NMEA 0183	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]
OpenPLC	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]
OpenSearch	Scenario	Infrastructure		RTE	TE	TB	2023-07	[99]
Podman	Computing Platform	Containerisation		RTE	TE	TB	2023-07	[99]
Yandex.Dialogs	Scenario	Infrastructure	E		TE	CR	2023-10	[213]
Iptables/nftables	Scenario	Infrastructure	E		TE	CR	2021-08	[93]
JSON	Scenario	Create/Edit	E		TE	CR	2021-08	[93]
LaZagne	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2021-08	[93]
Lets Encrypt	Scenario	Infrastructure	E		TE	CR	2021-08	[93]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	E		TE	CR	2021-08	[93]
opendns	Scenario	Infrastructure	E		TE	CR	2021-08	[93]
OpenSSH	Red Team Operations	Attack Strategy & Support	E		TE	CR	2021-08	[93]
OSSEC	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E		TE	CR	2021-08	[93]
Prelude	Blue Team Operations	SIEM & Security Analytics	E		TE	CR	2021-08	[93]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E		TE	CR	2021-08	[93]
Vagrant	Computing Platform	Infrastructure Provisioning and Configuration	E		TE	CR	2021-08	[93]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor	E		TE	CR	2021-08	[93]
OWASP Juice Shop	Red Team Operations	Training and Practice Systems		RTE		TB	2025-01	[23]
PhishDetector	Blue Team Operations	Phishing and Social Engineering		RTE		TB	2025-01	[23]
PhishTor	Blue Team Operations	Phishing and Social Engineering		RTE		TB	2025-01	[23]
ZPhisher	Red Team Operations	Phishing and Social Engineering		RTE		TB	2025-01	[23]
DIgSILENT PowerFactory	Scenario	Simulation and Emulation		RTE		TB	2024-10	[153]
DNP3	Scenario	Infrastructure		RTE		TB	2024-10	[153]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-10	[153]
Matrikon OPC	Scenario	Infrastructure		RTE		TB	2024-10	[153]
Triangle Microworks DTM	Scenario	Infrastructure		RTE		TB	2024-10	[153]
Burp	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2022-05	[206]
CTFd	Red Team Operations	Training and Practice Systems	E		TE	CR	2022-05	[206]
Datalog	Custom Development	Programming language	E		TE	CR	2022-05	[206]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2022-05	[206]
Immunity Debugger	Red Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2022-05	[206]
JSON	Scenario	Create/Edit	E		TE	CR	2022-05	[206]
Metasploit	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2022-05	[206]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	E		TE	CR	2022-05	[206]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2022-05	[206]
Wireshark	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2022-05	[206]
Freesweep	Red Team Operations	Attack Strategy & Support		RTE	TE	TB	2024-06	[52]
Iptables/nftables	Red Team Operations	Attack Strategy & Support		RTE	TE	TB	2024-06	[52]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2024-06	[52]
Modbus	Scenario	Infrastructure		RTE	TE	TB	2024-06	[52]
Netdiscover	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2024-06	[52]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2024-06	[52]
OpenPLC/OpenPLC Editor	Scenario	Create/Edit		RTE	TE	TB	2024-06	[52]
PfSense	Scenario	Infrastructure		RTE	TE	TB	2024-06	[52]
PyModbus	Scenario	Infrastructure		RTE	TE	TB	2024-06	[52]
ScadaBR	Scenario	Infrastructure		RTE	TE	TB	2024-06	[52]
VICSORT virtual testbed	Computing Platform	Integrated Testbed Solutions		RTE	TE	TB	2024-06	[52]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2024-06	[52]
EPANET	Scenario	Simulation and Emulation		RTE		TB	2025-02	[198]
NIST Randomness Test Suite	Blue Team Operations	Vulnerability Management		RTE		TB	2025-02	[198]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[198]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-03	[108]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-03	[108]
OpenPDC	Scenario	Infrastructure		RTE		TB	2024-03	[108]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
scapy	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[108]
Tcpdump	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[108]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[108]
Ansible	Computing Platform	Software Provisioning and Configuration			TE	CR	2021-08	[16]
Apache web server	Red Team Operations	Training and Practice Systems			TE	CR	2021-08	[16]
Vagrant	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2021-08	[16]
YAML	Scenario	Create/Edit			TE	CR	2021-08	[16]
CIC-IDS2017	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
CIC-IDS2018	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
ISCXVPN2016	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
Keras	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-07	[95]
P4 BMv2 software switch	Scenario	Infrastructure		RTE		TB	2025-07	[95]
P4 Compiler	Custom Development	Build-Toolchain		RTE		TB	2025-07	[95]
P4Utils	Scenario	Infrastructure		RTE		TB	2025-07	[95]
Tcpreplay	Scenario	Infrastructure		RTE		TB	2025-07	[95]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
ToN-IoT	Custom Development	AI & Machine Learning		RTE		TB	2025-07	[95]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-07	[95]
Bridge Command (BC)	Scenario	Simulation and Emulation		RTE		TB	2022-08	[205]
NMEA 0183	Scenario	Infrastructure		RTE		TB	2022-08	[205]
OpenCPN	Scenario	Simulation and Emulation		RTE		TB	2022-08	[205]
scapy	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2022-08	[205]
DNP3	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
GE eTerra PhasorPoint	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
GOOSE	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
MMS	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
Opal-RT Simulator	Scenario	Simulation and Emulation	E	RTE	TE	TB	2020-10	[144]
OpenPDC	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
PfSense	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
SIEMENS SICAM PAS	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[144]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E	RTE	TE	TB	2020-10	[144]
Suricata	Blue Team Operations	Firewalls & Network Security Gateways	E	RTE	TE	TB	2020-10	[144]
untangle	Blue Team Operations	Firewalls & Network Security Gateways	E	RTE	TE	TB	2020-10	[144]
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E	RTE	TE	TB	2020-10	[144]
5Greplay	Scenario	Infrastructure		RTE	TE	CR	2024-07	[58]
Free5GC	Scenario	Infrastructure		RTE	TE	CR	2024-07	[58]
Open5GS	Scenario	Infrastructure		RTE	TE	CR	2024-07	[58]
UERANSIM	Scenario	Infrastructure		RTE	TE	CR	2024-07	[58]
CSV	Scenario	Create/Edit		RTE		TB	2025-02	[201]
CyberVAN	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-02	[201]
Elastic Beats	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[201]
MySQL Database	Red Team Operations	Training and Practice Systems		RTE		TB	2025-02	[201]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2025-02	[201]
MATLAB/Simulink	Scenario	Infrastructure				TB	2023-12	[148]
MongoDB	Scenario	Infrastructure				TB	2023-12	[148]
CIS Ubuntu Security Guide	Blue Team Operations	Security Hardening		RTE		TB	2024-12	[86]
Clang-tidy	Blue Team Operations	Vulnerability Management		RTE		TB	2024-12	[86]
ike-scan	Blue Team Operations	Vulnerability Management		RTE		TB	2024-12	[86]
IPsec / IKEv2	Blue Team Operations	Firewalls & Network Security Gateways		RTE		TB	2024-12	[86]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[86]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[86]
O-DU-L2	Scenario	Simulation and Emulation		RTE		TB	2024-12	[86]
OWASP ASVS	Blue Team Operations	Vulnerability Management		RTE		TB	2024-12	[86]
ArduPilot	Scenario	Simulation and Emulation		RTE		TB	2024-12	[113]
CSV	Scenario	Infrastructure		RTE		TB	2024-12	[113]
Docker	Computing Platform	Containerisation		RTE		TB	2024-12	[113]
InfluxDB	Data Storage	Time-series database		RTE		TB	2024-12	[113]
iPerf	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-12	[113]
Keysight Open RAN Architect (KORA)	Scenario	Infrastructure		RTE		TB	2024-12	[113]
Kubernetes	Scenario	Infrastructure		RTE		TB	2024-12	[113]
Matlabs 4G toolbox	Scenario	Infrastructure		RTE		TB	2024-12	[113]
Matlabs 5G toolbox	Scenario	Infrastructure		RTE		TB	2024-12	[113]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MAVLink	Scenario	Infrastructure		RTE		TB	2024-12	[113]
NSF POWDER Wireless platform	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-12	[113]
srsRAN	Scenario	Infrastructure		RTE		TB	2024-12	[113]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2024-12	[113]
CVSS	Blue Team Operations	Vulnerability Management		RTE		CR	2024-09	[80]
Microsoft CyberBattleSim	Computing Platform	Integrated Testbed Solutions		RTE		CR	2024-09	[80]
PfSense	Scenario	Infrastructure		RTE		CR	2024-07	[195]
Skytap	Computing Platform	Cloud Infrastructure		RTE		CR	2024-07	[195]
Splunk	Blue Team Operations	SIEM & Security Analytics		RTE		CR	2024-07	[195]
Windows Task Scheduler	Scenario	Simulation and Emulation		RTE		CR	2024-07	[195]
Wordpress	Management	Content and Document Management		RTE		CR	2024-07	[195]
XAMPP	Scenario	Infrastructure		RTE		CR	2024-07	[195]
gym-pybullet-drones	Scenario	Simulation and Emulation		RTE		TB	2024-11	[197]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-11	[197]
Optuna	Custom Development	AI & Machine Learning		RTE		TB	2024-11	[197]
PyBullet Physics Engine	Scenario	Simulation and Emulation		RTE		TB	2024-11	[197]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2024-11	[197]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-11	[197]
Apache web server	Red Team Operations	Training and Practice Systems		RTE		TB	2025-05	[142]
Aposemat IoT-23 Dataset	Scenario	Infrastructure		RTE		TB	2025-05	[142]
CICIOT-2023	Scenario	Infrastructure		RTE		TB	2025-05	[142]
CSV	Custom Development	Dataset Generation		RTE		TB	2025-05	[142]
DPKT	Custom Development	Dataset Generation		RTE		TB	2025-05	[142]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-05	[142]
P4 BMv2 software switch	Scenario	Infrastructure		RTE		TB	2025-05	[142]
P4Utils	Scenario	Infrastructure		RTE		TB	2025-05	[142]
Pandas	Custom Development	Dataset Generation		RTE		TB	2025-05	[142]
scapy	Monitoring and Analytics	Data Collection		RTE		TB	2025-05	[142]
Slowloris	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-05	[142]
Tcpreplay	Monitoring and Analytics	Data Collection		RTE		TB	2025-05	[142]
CyRIS	Computing Platform	Infrastructure Instantiation Systems		RTE		CR	2025-01	[121]
Iptables/nftables	Network Infrastructure	Firewall and routing platform		RTE		CR	2025-01	[121]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2025-01	[121]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2025-01	[121]

Table 18 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-01	[121]
pymetasploit3	Red Team Operations	Attack Strategy & Support		RTE		CR	2025-01	[121]
python-nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-01	[121]
YAML	Scenario	Create/Edit		RTE		CR	2025-01	[121]
Apache JMeter	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[159]
cpprestsdk	Custom Development	Simulation Environment		RTE		TB	2025-04	[159]
Docker	Computing Platform	Containerisation		RTE		TB	2025-04	[159]
Hyperledger Composer	Scenario	Infrastructure		RTE		TB	2025-04	[159]
Hyperledger Fabric	Scenario	Infrastructure		RTE		TB	2025-04	[159]
Node.js	Custom Development	Backend Frameworks		RTE		TB	2025-04	[159]
ProVerif	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[159]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2025-04	[159]
VENTOS	Scenario	Simulation and Emulation		RTE		TB	2025-04	[159]
Ansible	Computing Platform	Software Provisioning and Configuration	E		TE	CR	2024-03	[63]
ELK Stack	Blue Team Operations	SIEM & Security Analytics	E		TE	CR	2024-03	[63]
Hydra	Red Team Operations	Brute force attacks	E		TE	CR	2024-03	[63]
John The Ripper	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2024-03	[63]
Kibana	Monitoring and Analytics	Visualization & Dashboarding	E		TE	CR	2024-03	[63]
LinPEAS	Red Team Operations	Vulnerability Management	E		TE	CR	2024-03	[63]
MITRE ATT&CK	Blue Team Operations	Threat Intelligence	E		TE	CR	2024-03	[63]
Moodle	Management	Learning Management System	E		TE	CR	2024-03	[63]
OpenSSH	Portal Services	User Access	E		TE	CR	2024-03	[63]
Packer	Computing Platform	Infrastructure Provisioning and Configuration	E		TE	CR	2024-03	[63]
ProM	Monitoring and Analytics	Data Collection	E		TE	CR	2024-03	[63]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration	E		TE	CR	2024-03	[63]
Windows Remote desktop protocol (RDP)	Portal Services	User Access	E		TE	CR	2024-03	[63]
Controller Area Network (CAN)	Scenario	Infrastructure		RTE		TB	2025-01	[202]
MQTT	Scenario	Infrastructure		RTE		TB	2025-01	[202]
OpenTAP	Scenario	Controlling		RTE		TB	2025-01	[202]
PASTA (Portable Automotive Security Testbed with Adaptability)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-01	[202]
Unity3D	Scenario	Simulation and Emulation		RTE		TB	2025-01	[202]

Table 19 Data repository (Part 6/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2021-04	[199]
OPNET	Network Infrastructure	Network Virtualization		RTE		TB	2021-04	[199]
RT-LAB	Scenario	Simulation and Emulation		RTE		TB	2021-04	[199]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2021-12	[165]
JSON	Scenario	Infrastructure		RTE		TB	2021-12	[165]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2021-12	[165]
Modbus	Scenario	Infrastructure		RTE		TB	2021-12	[165]
MQTT	Scenario	Infrastructure		RTE		TB	2021-12	[165]
Node-RED	Custom Development	Integrated Development Environment		RTE		TB	2021-12	[165]
DNP3	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[173]
GRFICS	Scenario	Simulation and Emulation	E	RTE	TE	TB	2024-12	[173]
Ignition SCADA	Custom Development	Visualization & Dashboarding	E	RTE	TE	TB	2024-12	[173]
Modbus	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[173]
NETLAB+	Portal Services	User Access	E	RTE	TE	TB	2024-12	[173]
OPC Unified Architecture (OPC-UA)	Custom Development	Visualization & Dashboarding	E	RTE	TE	TB	2024-12	[173]
OpenPLC	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[173]
Typhoon-HIL	Scenario	Simulation and Emulation	E	RTE	TE	TB	2024-12	[173]
VMWare ESXi	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE	TE	TB	2024-12	[173]
ANSYS	Scenario	Infrastructure		RTE		TB	2020-06	[210]
MATLAB/Simulink	Scenario	Infrastructure		RTE		TB	2020-06	[210]
Opal-RT Simulator	Scenario	Infrastructure		RTE		TB	2020-06	[210]
Docker	Computing Platform	Containerisation		RTE		CR	2025-03	[215]
Node.js	Scenario	Create/Edit		RTE		CR	2025-03	[215]
Npm	Scenario	Create/Edit		RTE		CR	2025-03	[215]
OSV Open Source Vulnerability	Scenario	Create/Edit		RTE		CR	2025-03	[215]
PyPI		Create/Edit		RTE		CR	2025-03	[215]
Elasticsearch	Blue Team Operations	SIEM & Security Analytics	E	RTE	TE	TB	2022-10	[49]
Kibana	Blue Team Operations	SIEM & Security Analytics	E	RTE	TE	TB	2022-10	[49]
Microsoft Hyper-V	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE	TE	TB	2022-10	[49]
Nmap	Blue Team Operations	Network Analysis & Reconnaissance	E	RTE	TE	TB	2022-10	[49]
OpenVAS	Blue Team Operations	Vulnerability Management	E	RTE	TE	TB	2022-10	[49]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
osquery	Monitoring and Analytics	Analysis & Verification	E	RTE	TE	TB	2022-10	[49]
Shodan	Blue Team Operations	Network Analysis & Reconnaissance	E	RTE	TE	TB	2022-10	[49]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E	RTE	TE	TB	2022-10	[49]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E	RTE	TE	TB	2022-10	[49]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE		TB	2021-12	[188]
Elastic Auditbeat	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[188]
Elastic Logstash	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[188]
Elasticsearch	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[188]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2021-12	[188]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-12	[188]
Microsoft Sysmon	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[188]
Mimikatz	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2021-12	[188]
Packer	Computing Platform	Infrastructure Provisioning and Configuration		RTE		TB	2021-12	[188]
Packetbeat	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[188]
Reg	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-12	[188]
Selenium	Scenario	User behaviour Simulation		RTE		TB	2021-12	[188]
Sigma	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-12	[188]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-12	[188]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2021-12	[188]
Tcpreplay	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[188]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2021-12	[188]
Xcopy	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-12	[188]
BB84	Scenario	Infrastructure		RTE		TB	2024-09	[137]
MATLAB	Scenario	Infrastructure		RTE		TB	2024-09	[137]
NS3	Scenario	Simulation and Emulation		RTE		TB	2024-09	[137]
OpenVirteX	Scenario	Infrastructure		RTE		TB	2024-09	[137]
QKDNetSim	Scenario	Simulation and Emulation		RTE		TB	2024-09	[137]
Ryu	Scenario	Infrastructure		RTE		TB	2024-09	[137]
TapBridge	Scenario	Infrastructure		RTE		TB	2024-09	[137]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
DNP3	Scenario	Infrastructure		RTE		TB	2021-10	[116]
MATPOWER	Scenario	Simulation and Emulation		RTE		TB	2021-10	[116]
NS3	Scenario	Infrastructure		RTE		TB	2021-10	[116]
PingThings Berkeley Tree Database (BTrDB)	Data Storage	Time-series database		RTE		TB	2021-10	[116]
PSSE	Scenario	Simulation and Emulation		RTE		TB	2021-10	[116]
RTDS	Scenario	Simulation and Emulation		RTE		TB	2021-10	[116]
Splunk	Monitoring and Analytics	Log Management		RTE		TB	2021-10	[116]
ABB Automation Builder IDE	Custom Development	Integrated Development Environment		RTE		TB	2025-01	[44]
Docker	Computing Platform	Containerisation		RTE		TB	2025-01	[44]
FUXA	Custom Development	Integrated Development Environment		RTE		TB	2025-01	[44]
Modbus	Scenario	Infrastructure		RTE		TB	2025-01	[44]
MulVAL	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-01	[44]
Node-RED	Custom Development	Infrastructure		RTE		TB	2025-01	[44]
pyModbus	Custom Development	Backend Frameworks		RTE		TB	2025-01	[44]
scapy	Red Team Operations	Paketmanipulation		RTE		TB	2025-01	[44]
cAdvisor	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[92]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2024-09	[92]
Hyperledger Fabric	Scenario	Infrastructure		RTE		TB	2024-09	[92]
IPFS	Data Storage	File & Block Storage		RTE		TB	2024-09	[92]
Ipfs Kubo	Data Storage	File & Block Storage		RTE		TB	2024-09	[92]
Node Exporter	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[92]
Prometheus	Monitoring and Analytics	Assets Monitoring		RTE		TB	2024-09	[92]
Simulated Ship Environment	Scenario	Simulation and Emulation		RTE		TB	2024-09	[92]
AWS IoT Greengrass	Scenario	Infrastructure		RTE		TB	2025-05	[59]
AWS QuickSight	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-05	[59]
AWS S3	Data Storage	Object Storage		RTE		TB	2025-05	[59]
edgeOps Benchmarking Tool	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-05	[59]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-05	[59]
Arpspoof	Red Team Operations	Paketmanipulation		RTE		TB	2024-12	[43]
Docker	Computing Platform	Containerisation		RTE		TB	2024-12	[43]
ELK Stack	Monitoring and Analytics	Log Management		RTE		TB	2024-12	[43]
JSON	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[43]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Modbus	Scenario	Infrastructure		RTE		TB	2024-12	[43]
Node-RED	Custom Development	Visualization & Dashboarding		RTE		TB	2024-12	[43]
OpenSSH	Portal Services	User Access		RTE		TB	2024-12	[43]
PyModbus	Scenario	Infrastructure		RTE		TB	2024-12	[43]
Tcpdump	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[43]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-12	[43]
Winlogbeat	Monitoring and Analytics	Log Management		RTE		TB	2024-12	[43]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[43]
Docker	Computing Platform	Containerisation		RTE		TB	2025-08	[184]
Iptables/nftables	Scenario	Infrastructure		RTE		TB	2025-08	[184]
Modbus	Scenario	Infrastructure		RTE		TB	2025-08	[184]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-08	[184]
PyCryptodome	Scenario	Create/Edit		RTE		TB	2025-08	[184]
pyModbus	Scenario	Infrastructure		RTE		TB	2025-08	[184]
scapy	Scenario	Infrastructure		RTE		TB	2025-08	[184]
tc netem	Scenario	Infrastructure		RTE		TB	2025-08	[184]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2024-08	[83]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		CR	2024-08	[83]
MQTT	Scenario	Infrastructure		RTE		CR	2024-08	[83]
Node-RED	Monitoring and Analytics	Visualization & Dashboarding		RTE		CR	2024-08	[83]
Wireshark	Red Team Operations	Paketmanipulation		RTE		CR	2024-08	[83]
ARINC 653 software emulator	Scenario	Simulation and Emulation		RTE		TB	2020-05	[131]
Binary Ninja	Custom Development	Reverse Engineering and Binary Analysis		RTE		TB	2020-05	[131]
CARLA	Scenario	Simulation and Emulation		RTE		TB	2020-05	[131]
CUDA	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[131]
Mambo	Scenario	Infrastructure		RTE		TB	2020-05	[131]
Mcsema	Scenario	Infrastructure		RTE		TB	2020-05	[131]
SVF library	Scenario	Infrastructure		RTE		TB	2020-05	[131]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[131]
Tensorflow Lite	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[131]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2020-05	[131]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE	TE	CR	2022-08	[94]
Arpspoof	Red Team Operations	Paketmanipulation		RTE	TE	CR	2022-08	[94]
DLMS/COSEM	Scenario	Infrastructure		RTE	TE	CR	2022-08	[94]
GIT	Management	Asset & Infrastructure Management		RTE	TE	CR	2022-08	[94]
Gurux	Scenario	Infrastructure		RTE	TE	CR	2022-08	[94]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
OpenStack	Computing Platform	Cloud Infrastructure		RTE	TE	CR	2022-08	[94]
Tcpdump	Red Team Operations	Attack Strategy & Support		RTE	TE	CR	2022-08	[94]
YAML	Scenario	Create/Edit		RTE	TE	CR	2022-08	[94]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE	TE	CR	2022-06	[3]
Apache web server	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2022-06	[3]
Contrast Security	Blue Team Operations	Application Security Testing		RTE	TE	CR	2022-06	[3]
Docker	Computing Platform	Containerisation		RTE	TE	CR	2022-06	[3]
DVWA	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2022-06	[3]
GNS3	Network Infrastructure	Network Virtualization		RTE	TE	CR	2022-06	[3]
Infection Monkey	Red Team Operations	Adversary emulation		RTE	TE	CR	2022-06	[3]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	CR	2022-06	[3]
Nessus	Blue Team Operations	Vulnerability Management		RTE	TE	CR	2022-06	[3]
Nikto	Blue Team Operations	Vulnerability Management		RTE	TE	CR	2022-06	[3]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	CR	2022-06	[3]
Owasp WebGoat	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2022-06	[3]
Owasp Zap (Zed Attack Proxy)	Blue Team Operations	Vulnerability Management		RTE	TE	CR	2022-06	[3]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE	TE	CR	2022-06	[3]
Wordpress	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2022-06	[3]
Free5GC	Scenario	Infrastructure		RTE		TB	2020-04	[112]
MANO	Scenario	Infrastructure		RTE		TB	2020-04	[112]
ONOS	Scenario	Infrastructure		RTE		TB	2020-04	[112]
OpenFlow	Scenario	Infrastructure		RTE		TB	2020-04	[112]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2020-04	[112]
scapy	Red Team Operations	Paketmanipulation		RTE		TB	2020-04	[112]
sFlow	Monitoring and Analytics	Analysis & Verification		RTE		TB	2020-04	[112]
URLhaus	Blue Team Operations	Malware Analysis		RTE		TB	2020-04	[112]
YAML	Scenario	Infrastructure		RTE		TB	2020-04	[112]
Zeek	Monitoring and Analytics	Analysis & Verification		RTE		TB	2020-04	[112]
Gephi	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-01	[29]
osquery	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-01	[29]
OSSEC	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-01	[29]
PostgreSQL	Data Storage	Relational Database		RTE		TB	2025-01	[29]
QEMU	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-01	[29]
rsyslog	Monitoring and Analytics	Log Management		RTE		TB	2025-01	[29]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Vulnerability Reproduction Tool (VRT)	Scenario	Infrastructure		RTE		TB	2025-01	[29]
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-01	[29]
curl-loader	Scenario	Traffic Generation		RTE		TB	2025-02	[141]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-02	[141]
Keras	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[141]
Matplotlib	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-02	[141]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-02	[141]
NetworkX	Scenario	Infrastructure		RTE		TB	2025-02	[141]
NumPy	Custom Development	Data Science		RTE		TB	2025-02	[141]
OpenFlow	Scenario	Infrastructure		RTE		TB	2025-02	[141]
Pandas	Custom Development	Data Science		RTE		TB	2025-02	[141]
Ryu	Scenario	Infrastructure		RTE		TB	2025-02	[141]
Seaborn	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[141]
Tcpdump	Monitoring and Analytics	Data Collection		RTE		TB	2025-02	[141]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[141]
Tshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-02	[141]
MITRE ATT&CK	Blue Team Operations	Threat Intelligence		RTE		TB	2025-01	[152]
MITRE Caldera	Red Team Operations	Adversary emulation		RTE		TB	2025-01	[152]
MulVAL	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-01	[152]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-01	[152]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2025-01	[152]
Windows Active Directory	Portal Services	Identity & Access Management (IAM)		RTE		TB	2025-01	[152]
IEC 60870-5-104	Scenario	Infrastructure		RTE		TB	2025-06	[194]
IPAL Toolset	Custom Development	Dataset Generation		RTE		TB	2025-06	[194]
PowerOwl	Scenario	Simulation and Emulation		RTE		TB	2025-06	[194]
Simbench	Scenario	Infrastructure		RTE		TB	2025-06	[194]
Wattson	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-06	[194]
Cyber Physical Systems Wind Tunnel (CPSWT)	Scenario	Simulation and Emulation		RTE		TB	2020-09	[119]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2020-09	[119]
InfluxDB	Data Storage	Time-series database		RTE		TB	2020-09	[119]

Table 19 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2020-09	[119]
SocketCAN	Scenario	Infrastructure		RTE		TB	2020-09	[119]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2020-09	[119]
V2X	Scenario	Simulation and Emulation		RTE		TB	2020-09	[119]
Veins	Scenario	Simulation and Emulation		RTE		TB	2020-09	[119]
WebGME	Scenario	Controlling		RTE		TB	2020-09	[119]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2020-09	[119]
ABB Robot Studio	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-02	[103]
COMAU PickApp HMI	Scenario	Simulation and Emulation		RTE		TB	2021-02	[103]
Kuka.Sim	Scenario	Simulation and Emulation		RTE		TB	2021-02	[103]
Modbus	Scenario	Infrastructure		RTE		TB	2021-02	[103]
S7comm	Scenario	Infrastructure		RTE		TB	2021-02	[103]
Anaconda	Custom Development	AI & Machine Learning		RTE		TB	2025-04	[191]
Apache Spark	Custom Development	AI & Machine Learning		RTE		TB	2025-04	[191]
CICFlowMeter	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[191]
CSV	Scenario	Infrastructure		RTE		TB	2025-04	[191]
Jupyter notebook	Custom Development	Integrated Development Environment		RTE		TB	2025-04	[191]
NumPy	Custom Development	Data Science		RTE		TB	2025-04	[191]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[191]
XAMPP	Scenario	Infrastructure		RTE		TB	2025-04	[191]
GOOSE	Scenario	Infrastructure		RTE		CR	2024-05	[22]
MMS	Scenario	Infrastructure		RTE		CR	2024-05	[22]
Pandapower	Scenario	Simulation and Emulation		RTE		CR	2024-05	[22]
Docker	Computing Platform	Containerisation	E		TE	CR	2020-10	[125]
Docker Hub	Computing Platform	Infrastructure Provisioning and Configuration	E		TE	CR	2020-10	[125]
Docker Swarm	Computing Platform	Container Orchestration	E		TE	CR	2020-10	[125]
DVWA	Red Team Operations	Training and Practice Systems	E		TE	CR	2020-10	[125]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure	E		TE	CR	2024-09	[64]

Table 20 Data repository (Part 7/7)

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Ansible	Computing Platform	Software Provisioning and Configuration			TE	CR	2024-09	[64]
Elastic Agent	Monitoring and Analytics	Data Collection			TE	CR	2024-09	[64]
Elastic Security (SIEM)	Blue Team Operations	SIEM & Security Analytics			TE	CR	2024-09	[64]
JSON	Scenario	Create/Edit			TE	CR	2024-09	[64]
Kibana	Monitoring and Analytics	Visualization & Dashboarding			TE	CR	2024-09	[64]
Libvirt	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2024-09	[64]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support			TE	CR	2024-09	[64]
MITRE Caldera	Red Team Operations	Adversary emulation			TE	CR	2024-09	[64]
Moodle	Management	Learning Management System			TE	CR	2024-09	[64]
OpenSSH	Portal Services	User Access			TE	CR	2024-09	[64]
Packer	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2024-09	[64]
Packetbeat	Monitoring and Analytics	Data Collection			TE	CR	2024-09	[64]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration			TE	CR	2024-09	[64]
Windows Remote desktop protocol (RDP)	Portal Services	User Access			TE	CR	2024-09	[64]
YAML	Scenario	Create/Edit			TE	CR	2024-09	[64]
Elasticsearch	Blue Team Operations	SIEM & Security Analytics		RTE		CR	2023-03	[27]
Endgame	Blue Team Operations	Endpoint Detection & Response (EDR)		RTE		CR	2023-03	[27]
Jira	Management	Operations Management		RTE		CR	2023-03	[27]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE		CR	2023-03	[27]
Nessus	Blue Team Operations	Vulnerability Management		RTE		CR	2023-03	[27]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		CR	2023-03	[27]
ThreatGrid	Blue Team Operations	Malware Analysis		RTE		CR	2023-03	[27]
VirusTotal	Blue Team Operations	Malware Analysis		RTE		CR	2023-03	[27]
Windows Active Directory	Management	Identity & Access Management (IAM)		RTE		CR	2023-03	[27]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2023-12	[96]
Mimikatz	Red Team Operations	Password Cracking and Credential Harvesting		RTE	TE	TB	2023-12	[96]
MMS	Scenario	Infrastructure		RTE	TE	TB	2023-12	[96]

Table 20 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Modbus	Scenario	Infrastructure		RTE	TE	TB	2023-12	[96]
scapy	Red Team Operations	Paketmanipulation		RTE	TE	TB	2023-12	[96]
Windows Remote desktop protocol (RDP)	Red Team Operations	Training and Practice Systems		RTE	TE	TB	2023-12	[96]
CSV	Custom Development	Dataset Generation		RTE		TB	2021-08	[84]
JSON	Management	Workflow & Orchestration		RTE		TB	2021-08	[84]
LoRa	Scenario	Infrastructure		RTE		TB	2021-08	[84]
Metasploit	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2021-08	[84]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		TB	2021-08	[84]
MQTT	Scenario	Infrastructure		RTE		TB	2021-08	[84]
MySQL Database	Data Storage	Relational Database		RTE		TB	2021-08	[84]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-08	[84]
Node-RED	Scenario	Infrastructure		RTE		TB	2021-08	[84]
OSSIM Alien Vault	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-08	[84]
PfSense	Network Infrastructure	Firewall and routing platform		RTE		TB	2021-08	[84]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2021-08	[84]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-08	[84]
sFuzz	Red Team Operations	Vulnerability Management		RTE		TB	2021-08	[84]
Tcpdump	Monitoring and Analytics	Data Collection		RTE		TB	2021-08	[84]
Thingsboard	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2021-08	[84]
Zeek	Monitoring and Analytics	Data Collection		RTE		TB	2021-08	[84]
ZigBee	Scenario	Infrastructure		RTE		TB	2021-08	[84]
ZigBee2MQTT	Scenario	Infrastructure		RTE		TB	2021-08	[84]
Z-Wave	Scenario	Infrastructure		RTE		TB	2021-08	[84]
Modbus	Red Team Operations	Training and Practice Systems		RTE	TE	TB	2022-03	[176]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2022-03	[176]
PsTools	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-03	[176]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance		RTE	TE	TB	2022-03	[176]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE		CR	2024-07	[24]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2024-07	[24]
OPNSense	Network Infrastructure	Firewall and routing platform		RTE		CR	2024-07	[24]
Pm4py	Management	Operations Management		RTE		CR	2024-07	[24]

Table 20 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
ProM	Management	Operations Management		RTE		CR	2024-07	[24]
Proxmox VE	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2024-07	[24]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration		RTE		CR	2024-07	[24]
Tracee	Monitoring and Analytics	Log Management		RTE		CR	2024-07	[24]
Vector	Monitoring and Analytics	Log Management		RTE		CR	2024-07	[24]
Acunetix	Scenario	Traffic Generation		RTE		TB	2024-09	[45]
Arachni	Scenario	Traffic Generation		RTE		TB	2024-09	[45]
DESLib (Dynamic Ensemble Selection Library)	Custom Development	Data Science		RTE		TB	2024-09	[45]
FlowTBag	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[45]
Honeyd	Blue Team Operations	Deception & Honeypot Systems		RTE		TB	2024-09	[45]
Iptables/nftables	Blue Team Operations	Firewalls & Network Security Gateways		RTE		TB	2024-09	[45]
Nessus	Scenario	Traffic Generation		RTE		TB	2024-09	[45]
Nmap	Scenario	Traffic Generation		RTE		TB	2024-09	[45]
NumPy	Custom Development	Data Science		RTE		TB	2024-09	[45]
Pandas	Custom Development	Data Science		RTE		TB	2024-09	[45]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[45]
scapy	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[45]
Smod	Scenario	Traffic Generation		RTE		TB	2024-09	[45]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-09	[45]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2024-08	[6]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2024-08	[6]
Veins	Scenario	Simulation and Emulation		RTE		TB	2024-08	[6]
WAVE protocol	Scenario	Infrastructure		RTE		TB	2024-08	[6]
INET	Scenario	Create/Edit		RTE		TB	2024-04	[5]
NETA	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-04	[5]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2024-04	[5]
Ponder2	Scenario	Infrastructure		RTE		TB	2024-04	[5]
PReSET	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[5]
ReaSE	Scenario	Create/Edit		RTE		TB	2024-04	[5]
SEA++	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[5]
Tribe Flood Network (TFN)	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-04	[5]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-04	[5]

Table 20 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
GOOSE	Scenario	Infrastructure		RTE		CR	2023-06	[106]
JSON	Scenario	Infrastructure		RTE		CR	2023-06	[106]
Mininet	Network Infrastructure	Network Virtualization		RTE		CR	2023-06	[106]
MMS	Scenario	Infrastructure		RTE		CR	2023-06	[106]
MySQL Database	Data Storage	Relational Database		RTE		CR	2023-06	[106]
OpenPLC	Scenario	Simulation and Emulation		RTE		CR	2023-06	[106]
Pandapower	Scenario	Simulation and Emulation		RTE		CR	2023-06	[106]
R-GOOSE	Scenario	Infrastructure		RTE		CR	2023-06	[106]
R-SV (Routable Sampled Value)	Scenario	Infrastructure		RTE		CR	2023-06	[106]
ScadaBR	Scenario	Infrastructure		RTE		CR	2023-06	[106]
XML	Scenario	Create/Edit		RTE		CR	2023-06	[106]
Docker	Computing Platform	Containerisation			TE	CR	2023-04	[61]
Dsiem	Blue Team Operations	SIEM & Security Analytics			TE	CR	2023-04	[61]
ELK Stack	Blue Team Operations	SIEM & Security Analytics			TE	CR	2023-04	[61]
Ettercap	Red Team Operations	Exploitation and Attack Execution			TE	CR	2023-04	[61]
Kibana	Blue Team Operations	SIEM & Security Analytics			TE	CR	2023-04	[61]
MiniCPS	Network Infrastructure	Network Virtualization			TE	CR	2023-04	[61]
Mininet	Network Infrastructure	Network Virtualization			TE	CR	2023-04	[61]
scapy	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)			TE	CR	2023-04	[61]
arp-scan	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[207]
CSV	Scenario	Infrastructure		RTE		CR	2022-09	[207]
Datalog	Custom Development	Programming language		RTE		CR	2022-09	[207]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2022-09	[207]
Mimikatz	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2022-09	[207]
nbtscan	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[207]
Netdiscover	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[207]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[207]
Norwegian Cyber Range	Computing Platform	Integrated Cyber Range Solutions		RTE		CR	2022-09	[207]
PyDatalog	Red Team Operations	Attack Strategy & Support		RTE		CR	2022-09	[207]
VNCDtool	Scenario	Traffic Generation		RTE		CR	2022-09	[207]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2022-08	[97]
NS3	Network Infrastructure	Network Virtualization		RTE		CR	2022-08	[97]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		CR	2022-08	[97]
Docker	Computing Platform	Containerisation		RTE		TB	2024-09	[48]

Table 20 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
ICSFlowGenerator	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[48]
ICSSIM Framework	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-09	[48]
JSON	Scenario	Infrastructure		RTE		TB	2024-09	[48]
Modbus	Scenario	Create/Edit		RTE		TB	2024-09	[48]
MQTT Broker	Red Team Operations	Training and Practice Systems		RTE		TB	2024-09	[48]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2024-06	[1]
Security Credential Management System (SCMS)	Management	Identity & Access Management (IAM)		RTE		TB	2024-06	[1]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2024-06	[1]
V2X	Scenario	Infrastructure		RTE		TB	2024-06	[1]
VENTOS	Scenario	Simulation and Emulation		RTE		TB	2024-06	[1]
Minimega	Computing Platform	Integrated Cyber Range Solutions				CR	2022-08	[181]
Nmap	Red Team Operations	Network Scanning and Reconnaissance				CR	2022-08	[181]
SCORCH	Scenario	Controlling				CR	2022-08	[181]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				CR	2022-08	[181]
INET	Scenario	Create/Edit		RTE		TB	2024-01	[172]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2024-01	[172]
Scyther	Blue Team Operations	Vulnerability Management		RTE		TB	2024-01	[172]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2024-01	[172]
Tamarin Prover	Scenario	Infrastructure		RTE		TB	2024-01	[172]
Veins	Scenario	Simulation and Emulation		RTE		TB	2024-01	[172]
Android Emulator	Scenario	Simulation and Emulation		RTE	TE	TB	2022-08	[204]
asn1c tool	Custom Development	Build-Toolchain		RTE	TE	TB	2022-08	[204]
Bettercap	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-08	[204]
Docker	Computing Platform	Containerisation		RTE	TE	TB	2022-08	[204]
Hydra	Red Team Operations	Brute force attacks		RTE	TE	TB	2022-08	[204]
JupyterHub	Portal Services	User Access		RTE	TE	TB	2022-08	[204]
Kubernetes	Computing Platform	Infrastructure Provisioning and Configuration		RTE	TE	TB	2022-08	[204]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-08	[204]
MongoDB	Data Storage	NoSQL Database		RTE	TE	TB	2022-08	[204]
OAIs gNB emulator	Scenario	Infrastructure		RTE	TE	TB	2022-08	[204]
OAuth 2.0	Portal Services	Identity & Access Management (IAM)		RTE	TE	TB	2022-08	[204]
Openapi-generator	Scenario	Infrastructure		RTE	TE	TB	2022-08	[204]
P4 BMv2 software switch	Scenario	Infrastructure		RTE	TE	TB	2022-08	[204]
sFuzz	Red Team Operations	Vulnerability Management		RTE	TE	TB	2022-08	[204]
Tcpdump	Monitoring and Analytics	Data Collection		RTE	TE	TB	2022-08	[204]

Table 20 continued

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
wfuzz	Red Team Operations	Vulnerability Management		RTE	TE	TB	2022-08	[204]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2022-08	[204]
Controller Area Network (CAN)	Scenario	Infrastructure		RTE		TB	2023-07	[211]
LIN	Scenario	Infrastructure		RTE		TB	2023-07	[211]
SavvyCan	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[211]
scapy	Red Team Operations	Vulnerability Management		RTE		TB	2023-07	[211]
TSMaster	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[211]
VXDIAG VCX Professional Car Diagnostic	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[211]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[211]
Docker	Computing Platform	Containerisation		RTE		TB	2025-06	[186]
Helm	Computing Platform	Container Orchestration		RTE		TB	2025-06	[186]
Kubernetes	Scenario	Infrastructure		RTE		TB	2025-06	[186]
MITRE CAPEC	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[186]
MITRE CWE	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[186]
NumPy	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[186]
NVD	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[186]
O-RAN SC	Scenario	Infrastructure		RTE		TB	2025-06	[186]
Pandas	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[186]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[186]
Transformers	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[186]
Trivy	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[186]
Google Cloud	Computing Platform	Cloud Infrastructure	E	RTE		TB	2021-04	[82]
Modbus	Scenario	Infrastructure	E	RTE		TB	2021-04	[82]
modpoll	Scenario	Traffic Generation	E	RTE		TB	2021-04	[82]
OpenPLC	Scenario	Infrastructure	E	RTE		TB	2021-04	[82]
PfSense	Blue Team Operations	Firewalls & Network Security Gateways	E	RTE		TB	2021-04	[82]
PyModbus	Scenario	Infrastructure	E	RTE		TB	2021-04	[82]
ScadaBR	Scenario	Infrastructure	E	RTE		TB	2021-04	[82]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE		TB	2021-04	[82]
Windows Active Directory	Management	Identity & Access Management (IAM)	E	RTE		TB	2021-04	[82]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E	RTE		TB	2021-04	[82]

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10207-026-01298-y.

Author Contributions K.M. conducted the literature review, screening, data extraction, categorization, and analysis, and wrote the main manuscript text. F.S., M.L., and M.W. contributed to the study design, methodology, interpretation of the results, and critical revision of the manuscript, and supervised the study. All authors reviewed and approved the final manuscript.

Funding Open access funding provided by AIT Austrian Institute of Technology GmbH. The work in this paper has received funding from the Austrian Research Promotion Agency (FFG) under GA no. FO999905294 (CyberTASTE).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflicts of Interest The authors declare that they have no conflict of interest.

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

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

References

1. Abdo, A., Wu, G., Abu-Ghazaleh, N.: VEhicular Secure Network Open Simulator (VESNOS): A Cyber-security oriented co-simulation platform for connected and automated driving. In: Proceedings of the 38th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation, SIGSIM-PADS '24, pp. 108–118. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3615979.3656054
2. Abu Waraga, O., Bettayeb, M., Nasir, Q., Abu Talib, M.: Design and implementation of automated IoT security testbed. Computers & Security **88**, 101648 (2020). https://doi.org/10.1016/j.cose.2019.101648
3. Acheampong, R., Bălan, T.C., Popovici, D.M., Rekeraho, A.: Security scenarios automation and deployment in virtual environment using ansible. In: 2022 14th International Conference on Communications (COMM), pp. 1–7 (2022). https://doi.org/10.1109/COMM54429.2022.9817150
4. Alasali, F., El-Naily, N., Holderbaum, W., Mustafa, H.Y., AlMajali, A., Itradat, A.: A hybrid physical and co-simulation modern adaptive power protection testbed for testing the resilience of smart grids under cyber-physical threats. Energy Rep. **12**, 1655–1672 (2024). https://doi.org/10.1016/j.egyr.2024.07.051
5. AlHidaifi, S.M., Asghar, M.R., Ansari, I.S.: Towards a cyber resilience quantification framework (CRQF) for IT infrastructure. Comput. Netw. **247**, 110446 (2024). https://doi.org/10.1016/j.comnet.2024.110446
6. Ali, W.A., Mangini, A.M., Júlvez, J., Mahulea, C., Fanti, M.P.: Toward enhancing security in intelligent transportation: A simulation-based approach. IFAC-PapersOnLine **58**(4), 156–161 (2024). https://doi.org/10.1016/j.ifacol.2024.07.210
7. Almazyad, I., Elmadani, S., Hariri, S.: A 5G and beyond testbed for cybersecurity research and education. In: 2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA), pp. 1–6 (2024). https://doi.org/10.1109/AICCSA63423.2024.10912627
8. Alnajim, A., Alotaibi, F., Khan, S.: Detecting and mitigating distributed denial of service attacks in software-defined networking. Computers, Materials and Continua **83**(3), 4515–4535 (2025). https://doi.org/10.32604/cmc.2025.063139
9. Alves, M.R.C., Rudie, K., Pena, P.N.: A security testbed for networked DES control systems. IFAC-PapersOnLine **55**(28), 128–134 (2022). https://doi.org/10.1016/j.ifacol.2022.10.334
10. Amponis, G., Radoglou-Grammatikis, P., Lagkas, T., Ouzounidis, S., Zevgara, M., Moscholios, I., Goudos, S., Sarigiannidis, P.: Generating full-stack 5G security datasets: IP-layer and core network persistent PDU session attacks. AEU-Int. J. Electron. C. **171**, 154913 (2023). https://doi.org/10.1016/j.aeue.2023.154913
11. Antonopoulos, M., Drainakis, G., Ouzounoglou, E., Papavassiliou, G., Amditis, A.: Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain. In: 2022 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 305–310 (2022). https://doi.org/10.1109/CSR54599.2022.9850280
12. Baral, S., Saha, S., Haque, A.: Autonomous cyber incident response using reasoning and action. In: 2025 International Wireless Communications and Mobile Computing (IWCMC), pp. 1392–1397 (2025). https://doi.org/10.1109/IWCMC65282.2025.11059476
13. Bartusiak, A., Seidl, F., Lässig, J., Nicolai, S., Bretschneider, P.: Enhancing cyber resilience in energy systems through automated attack scenario generation: A toolchain approach. In: 2024 International Conference on Smart Energy Systems and Technologies (SEST), pp. 1–6 (2024). https://doi.org/10.1109/SEST61601.2024.10694631
14. Ben-Shimol, L., Lavi, D., Klevansky, E., Brodt, O., Mimran, D., Elovici, Y., Shabtai, A.: Detection of compromised functions in a serverless cloud environment. Computers & Security **150**, 104261 (2025). https://doi.org/10.1016/j.cose.2024.104261
15. Berg, T.H., Amro, A., Akbarzadeh, A., Kavallieratos, G.: From Words to Wires: Toward Rapid ICS Cyber-Range Construction Using LLMs. In: R. Laborde, J. Garcia-Alfaro, G. Navarro, J. Herrera-Joancomartí, H. Hartenstein, S. Katsikas, F. Cuppens (eds.) Computer Security. ESORICS 2025 International Workshops, pp. 462–481. Springer Nature Switzerland, Cham (2026). https://doi.org/10.1007/978-3-032-16089-8_28
16. Bernardinetti, G., Iafrate, S., Bianchi, G.: Nautilus: A tool for automated deployment and sharing of cyber range scenarios. In: Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, pp. 1–7. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3469182
17. Beuran, R., Vykopal, J., Belajová, D., Čeleda, P., Tan, Y., Shinoda, Y.: Capability assessment methodology and comparative analysis of cybersecurity training platforms. Computers & Security **128**, 103120 (2023). https://doi.org/10.1016/j.cose.2023.103120

18. Beuran, R., Wang, J., Zhao, M., Tan, Y.: IoT security training for system developers: Methodology and tools. Internet of Things **24**, 100931 (2023). https://doi.org/10.1016/j.iot.2023.100931
19. Beuran, R., Zhang, Z., Tan, Y.: AWS EC2 public cloud cyber range deployment. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 433–441 (2022). https://doi.org/10.1109/EuroSPW55150.2022.00051
20. Bhat, P., J, N.H., Mohana: Cyber security testbed: Keyloggers and data visualization on keyloggers - a case study. In: 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), pp. 216–221 (2023). https://doi.org/10.1109/ICSCNA58489.2023.10370136
21. Bierwirth, T., Pfützner, S., Schopp, M., Steininger, C.: Design and evaluation of advanced persistent threat scenarios for cyber ranges. IEEE access: practical innovations, open solutions **12**, 72458–72472 (2024). https://doi.org/10.1109/ACCESS.2024.3402744
22. Biswas, J., Godse, R., Chen, B., Roomi, M.M., Ng, B.: Substation simulation synchronization - towards a distributed and scaled power grid cyber range. In: The 15th ACM International Conference on Future and Sustainable Energy Systems, pp. 655–663. ACM (2024). https://doi.org/10.1145/3632775.3661992
23. Blancaflor, E.B., Lara, C.G.E., Mancilla, D.F.L., Caberto, D.J.V., Magno, F.D.C.: Mitigating injection and phishing attacks through input validation and phishing detection techniques. In: Proceeding of the 2024 6th International Conference on Information Technology and Computer Communications, ITCC '24, pp. 13–20. Association for Computing Machinery, New York, NY, USA (2025). https://doi.org/10.1145/3704391.3704394
24. Blefari, F., Pironti, F.A., Furfaro, A.: Toward a log-based anomaly detection system for cyber range platforms. In: Proceedings of the 19th International Conference on Availability, Reliability and Security, pp. 1–9. ACM (2024). https://doi.org/10.1145/3664476.3669976
25. Boeding, M., Hempel, M., Sharif, H., Lopez, J., Perumalla, K.: A flexible OT testbed for evaluating on-device implementations of IEC-61850 GOOSE. Int. J. Crit. Infrastruct. Prot. **42**, 100618 (2023). https://doi.org/10.1016/j.ijcip.2023.100618
26. Bonagura, V., Pisani, J., Ferrato, A., Foglietta, C., Cavone, G., Pascucci, F.: Machine Learning Techniques for Anomaly Detection in the Hydra Testbed: A Data-Driven Defense Strategy. In: G. Oliva, S. Panzieri, B. Hämmerli, F. Pascucci, L. Faramondi (eds.) Critical Information Infrastructures Security, pp. 343–361. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-84260-3_20
27. Bridges, R.A., Rice, A.E., Oesch, S., Nichols, J.A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S.C., Erwin, S.: Testing SOAR tools in use. Computers & Security **129**, 103201 (2023). https://doi.org/10.1016/j.cose.2023.103201
28. Busquime Silva, R.A., Piqueira, J.R.C., Cruz, J.J., Marques, R.P.: Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants. International Journal of Critical Infrastructure Protection **34**, 100453 (2021). https://doi.org/10.1016/j.ijcip.2021.100453
29. Cao, P., Kalbarczyk, Z., Iyer, R.K.: Security testbed for preempting attacks against supercomputing infrastructure. In: SC24-w: Workshops of the International Conference for High Performance Computing, Networking, Storage and Analysis, pp. 1781–1788. IEEE, Atlanta, GA, USA (2024). https://doi.org/10.1109/SCW63240.2024.00223
30. Capone, D., Caturano, F., Delicato, A., Perrone, G., Romano, S.P.: Dockerized Android: A container-based platform to build mobile Android scenarios for Cyber Ranges. In: 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1–9 (2022). https://doi.org/10.1109/ICECET55527.2022.9872834
31. Čeleda, P., Vykopal, J., Švábenský, V., Slavíček, K.: KYPO4INDUSTRY: A testbed for teaching cybersecurity of industrial control systems. In: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE '20, pp. 1026–1032. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3328778.3366908
32. Chandrashekar, N.D., King, K., Gračanin, D., Azab, M.: Design & development of virtual reality empowered cyber-security training testbed for IoT systems. In: 2023 3rd Intelligent Cybersecurity Conference (ICSC), pp. 86–94 (2023). https://doi.org/10.1109/ICSC60084.2023.10349976
33. Chen, X., Coble, J., Zhang, F.: A full-scope, high-fidelity simulator-based hardware-in-the-loop testbed for comprehensive nuclear power plant cybersecurity research. Prog. Nucl. Energy **175**, 105348 (2024). https://doi.org/10.1016/j.pnucene.2024.105348
34. Chianese, L., Granata, D., Palmiero, P., Rak, M.: Leveraging threat modelling for effective penetration testing in 5G systems. In: 2024 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 180–185 (2024). https://doi.org/10.1109/CSR61664.2024.10679437
35. Chng, B., Ng, B., Roomi, M.M., Mashima, D., Lou, X.: CRaaS: Cloud-based smart grid cyber range for scalable cybersecurity experiments and training. In: 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 333–339 (2024). https://doi.org/10.1109/SmartGridComm60555.2024.10738051
36. Choi, J., Narayanasamy, D., Ahn, B., Ahmad, S., Zeng, J., Kim, T.: A real-time hardware-in-the-loop (HIL) cybersecurity testbed for power electronics devices and systems in cyber-physical environments. In: 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), pp. 1–5 (2021). https://doi.org/10.1109/PEDG51384.2021.9494202
37. Chouliaras, N., Kantzavelou, I., Pantziou, G., Maglaras, L., Chouliara-Sidera, P., Adamakos, A., Chalatsakos, P.: ETHACA - a container-based cyber range for research and education. In: 2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6 (2024). https://doi.org/10.1109/CAMAD62243.2024.10942721
38. Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., Ferrag, M.A.: Cyber Ranges and TestBeds for Education, Training, and Research. Appl. Sci. **11**(4), 1809 (2021). https://doi.org/10.3390/app11041809
39. Colarusso, C., Falco, I., Zimeo, E.: Business continuity of Cloud-based IoT applications through a seamless continuum. Internet of Things **33**, 101723 (2025). https://doi.org/10.1016/j.iot.2025.101723
40. Cook, J., Weiss, R., Mache, J., Morán, C.G., Wang, J.: An authoring process to construct docker containers to help instructors develop cybersecurity exercises. J. Comput. Sci. Coll. **37**(10), 37–47 (2022)
41. Coshatt, S.J., Li, Q., Yang, B., Wu, S., Shrivastava, D., Ye, J., Song, W., Zahiri, F.: Design of cyber-physical security testbed for multi-stage manufacturing system. In: GLOBECOM 2022 - 2022 IEEE Global Communications Conference, pp. 1978–1983 (2022). https://doi.org/10.1109/GLOBECOM48099.2022.10000849
42. Cruz, T., Simões, P.: Down the Rabbit Hole: Fostering Active Learning through Guided Exploration of a SCADA Cyber Range. Appl. Sci. **11**(20), 9509 (2021). https://doi.org/10.3390/app11209509

43. Cuorvo, R., d'Ambrosio, N., Iorio, D., Perrone, G., Romano, S.P.: Securing industrial systems: A testbed for cyber-defense evaluation and data collection. In: 2024 20th International Conference on Network and Service Management (CNSM), pp. 1–7 (2024). https://doi.org/10.23919/CNSM62983.2024.10814599
44. d'Ambrosio, N., Capodagli, G., Perrone, G., Romano, S.P.: SCASS: Breaking into SCADA systems security. Computers & Security **151**, 104315 (2025). https://doi.org/10.1016/j.cose.2025.104315
45. de Oliveira, P.R., Viegas, E.K., Santin, A.O., Horchulhack, P., de Matos, E.: Toward a reliable network-based intrusion detection model for SCADA: A classification with reject option approach. In: 2024 International Joint Conference on Neural Networks (IJCNN), pp. 1–8 (2024). https://doi.org/10.1109/IJCNN60899.2024.10650735
46. Degefa, M.Z., Sanchez, S., Borgaonkar, R.: A testbed for advanced distribution management systems: Assessment of cybersecurity. In: 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1–5 (2021). https://doi.org/10.1109/ISGTEurope52324.2021.9640184
47. Dehlaghi-Ghadim, A., Balador, A., Moghadam, M.H., Hansson, H., Conti, M.: ICSSIM – A framework for building industrial control systems security testbeds. Comput. Ind. **148**, 103906 (2023). https://doi.org/10.1016/j.compind.2023.103906
48. Dehlaghi-Ghadim, A., Ericsson, N., Magnusson, L.G., Eriksson, M., Moghadam, M.H., Balador, A., Hansson, H.: Using decision support to fortify industrial control system against cyberattacks. In: 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–4 (2024). https://doi.org/10.1109/ETFA61755.2024.10710892
49. Domínguez, M., Pérez, D., Morán, A., Alonso, S., Prada, M.A., Fuertes, J.J.: Remote training in cybersecurity for industrial control systems. IFAC-PapersOnLine **55**(17), 320–325 (2022). https://doi.org/10.1016/j.ifacol.2022.09.299
50. Doussau, A., Souyris, C.C.P., Yamin, M.M., Katt, B., Ullah, M.: Intelligent contextualized network traffic generator in a cyber range. In: 2023 17th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp. 9–13 (2023). https://doi.org/10.1109/SITIS61268.2023.00012
51. Du, L., He, J., Li, T., Wang, Y., Lan, X., Huang, Y.: DBWE-Corbat: Background network traffic generation using dynamic word embedding and contrastive learning for cyber range. Computers & Security **129**, 103202 (2023). https://doi.org/10.1016/j.cose.2023.103202
52. Ekisa, C., Briain, D.Ó., Kavanagh, Y.: Modelling and simulating advanced cyber-threats to industrial control systems with an emulated testbed. In: 2024 35th Irish Signals and Systems Conference (ISSC), pp. 1–6 (2024). https://doi.org/10.1109/ISSC61953.2024.10603140
53. El-Sayed, A., Toony, A.A., Alqahtani, F., Alginahi, Y., Said, W.: CO-STOP: A robust P4-powered adaptive framework for comprehensive detection and mitigation of coordinated and multi-faceted attacks in SD-IoT networks. Computers & Security **151**, 104349 (2025). https://doi.org/10.1016/j.cose.2025.104349
54. El-Sayed, A., Toony, A.A., Tolba, A., Alqahtani, F., Alginahi, Y., Said, W.: Deception and cloud integration: A multi-layered approach for DDoS detection, mitigation, and attack surface minimization in SD-IoT networks. Comput. Electr. Eng. **126**, 110543 (2025). https://doi.org/10.1016/j.compeleceng.2025.110543
55. Erkek, Í., Irmak, E.: Evaluation of SCADA test beds and design of a new software-based test bed. In: 2023 11th International Conference on Smart Grid (icSmartGrid), pp. 1–8 (2023). https://doi.org/10.1109/icSmartGrid58556.2023.10170935
56. Escolar, A.M., Wang, Q., Calero, J.M.A.: Enhancing honeynet-based protection with network slicing for massive Pre-6G IoT Smart Cities deployments. J. Netw. Comput. Appl. **229**, 103918 (2024). https://doi.org/10.1016/j.jnca.2024.103918
57. European Cyber Security Organisation (ECSO): Understanding cyber ranges: From hype to reality. WG5 Paper SWG 5.1: Cyber Range Environments and Technical Exercises, European Cyber Security Organisation (ECSO), Brussels, Belgium (2020). https://ecs-org.eu/ecso-uploads/2023/05/2020_SWG-5.1_paper_UnderstandingCyberRanges_final_v1.0-update.pdf. Accessed 2025-11-12
58. Farao, A., Ntantogian, C., Karagiannis, S., Magkos, E., Dritsa, A., Xenakis, C.: NITRO: An interconnected 5G-IoT cyber range. In: Proceedings of the 19th International Conference on Availability, Reliability and Security, pp. 1–6. ACM (2024). https://doi.org/10.1145/3664476.3669919
59. Farjad, S.M., Patllola, S.R., Kassa, Y., Grispos, G., Gandhi, R.: Secure edge computing reference architecture for data-driven structural health monitoring: Lessons learned from implementation and benchmarking. In: Proceedings of the 2025 ACM Southeast Conference, pp. 145–154. ACM, Southeast Missouri State University Cape Girardeau MO USA (2025). https://doi.org/10.1145/3696673.3723074
60. Glas, M., Messmann, G., Pernul, G.: Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises. Computers & Security **144**, 103965 (2024). https://doi.org/10.1016/j.cose.2024.103965
61. Glas, M., Vielberth, M., Pernul, G.: Train as you fight: Evaluating authentic cybersecurity training in cyber ranges. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, pp. 1–19. ACM, Hamburg Germany (2023). https://doi.org/10.1145/3544548.3581046
62. Grasselli, C., Melis, A., Girau, R., Callegati, F.: A digital twin for enhanced cybersecurity in connected vehicles. In: 2023 23rd International Conference on Transparent Optical Networks (ICTON), pp. 1–4 (2023). https://doi.org/10.1109/ICTON59386.2023.10207369
63. Guerrero, G., Betarte, G., Campo, J.D.: Process mining-based assessment of cyber range trainings. In: 2024 L Latin American Computer Conference (CLEI), pp. 1–10 (2024). https://doi.org/10.1109/CLEI64178.2024.10700452
64. Guerrero, G., Betarte, G., Campo, J.D.: Tectonic: An academic cyber range. In: 2024 IEEE Biennial Congress of Argentina (ARGENCON), pp. 1–8 (2024). https://doi.org/10.1109/ARGENCON62399.2024.10735713
65. Gutiérrez Mlot, E.D., Saldana, J., Rodríguez, R.J., Kotsiuba, I., Gañán, C.: A dataset to train intrusion detection systems based on machine learning models for electrical substations. Data Brief **57**, 111153 (2024). https://doi.org/10.1016/j.dib.2024.111153
66. Hatcher, W., Harrison, T., Brown, T., Hammad, E.: CyberExpert: Towards an automated framework for cybersecurity expertise acquisition and mastery. In: 2023 IEEE Frontiers in Education Conference (FIE), pp. 1–7 (2023). https://doi.org/10.1109/FIE58773.2023.10343334
67. Huang, K., Zhou, C., Qin, Y., Tu, W.: A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems. IEEE Trans. Industr. Electron. **67**(3), 2371–2379 (2020). https://doi.org/10.1109/TIE.2019.2907451
68. Huff, P., Leiterman, S., Springer, J.P.: Cyber arena: An open-source solution for scalable cybersecurity labs in the cloud. In: Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1, SIGCSE 2023, pp. 221–227. Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3545945.3569828
69. Jørgensen, P.A., Waltoft-Olsen, A., Houmb, S.H., Toppe, A.L., Soltvedt, T.G., Muggerud, H.K.: Building a hardware-in-the-loop (HiL) digital energy station infrastructure for cyber operation resiliency testing. In: Proceedings of the 3rd International Work-

shop on Engineering and Cybersecurity of Critical Systems, EnCyCriS '22, pp. 9–16. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3524489.3527299
70. Kabbara, N., Cibin, N., Morais, H., Ştefanov, A., Gibescu, M.: A cybersecurity assessment for hybrid virtualized-physical digital substations. Sustainable Energy, Grids and Networks **43**, 101795 (2025). https://doi.org/10.1016/j.segan.2025.101795
71. Kampourakis, V., Gkioulos, V., Katsikas, S.: A step-by-step definition of a reference architecture for cyber ranges. Journal of Information Security and Applications **88**, 103917 (2025). https://doi.org/10.1016/j.jisa.2024.103917
72. Kampourakis, V., Kavallieratos, G., Spathoulas, G., Gkioulos, V., Katsikas, S.: LLM-Assisted AHP for Explainable Cyber Range Evaluation (2025). https://doi.org/10.48550/arXiv.2512.10487
73. Kampourakis, V., Takaronis, M., Gkioulos, V., Katsikas, S.: An Ontology-Based Framework for Semantic Representation of the Cyber Range Domain. Journal of Cybersecurity and Privacy **6**(2), 76 (2026). https://doi.org/10.3390/jcp6020076
74. Kandasamy, N.K., Venugopalan, S., Wong, T.K., Leu, N.J.: An electric power digital twin for cyber security testing, research and education. Comput. Electr. Eng. **101**, 108061 (2022). https://doi.org/10.1016/j.compeleceng.2022.108061
75. Karimi, M., Bartlett, S., Mena, D.M.: A testbed approach to assessing and mitigating iiot network vulnerabilities. In: 2025 13th International Conference on Smart Grid (icSmartGrid), pp. 1–5 (2025). https://doi.org/10.1109/icSmartGrid66138.2025.11071848
76. Katsantonis, M.N., Manikas, A., Mavridis, I., Gritzalis, D.: Cyber range design framework for cyber security education and training. Int. J. Inf. Secur. **22**(4), 1005–1027 (2023). https://doi.org/10.1007/s10207-023-00680-4
77. Kaur, S., Kumar, K., Aggarwal, N.: Enhancing DDoS defense in SDN using hierarchical machine learning models. J. Netw. Comput. Appl. **239**, 104168 (2025). https://doi.org/10.1016/j.jnca.2025.104168
78. Kavitha, D., Ramalakshmi, R.: Machine learning-based DDOS attack detection and mitigation in SDNs for IoT environments. J. Franklin Inst. **361**(17), 107197 (2024). https://doi.org/10.1016/j.jfranklin.2024.107197
79. Kellerer, N., Sánchez, G., Alberto, H., Hagenmeyer, V., Elbez, G.: Attacks on the siemens S7 protocol using an industrial control system testbed. In: Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems, E-Energy '25, pp. 770–779. Association for Computing Machinery, New York, NY, USA (2025). https://doi.org/10.1145/3679240.3734645
80. Kim, B.S., Suk, H.W., Choi, Y.H., Moon, D.S., Kim, M.S.: Optimal cyber attack strategy using reinforcement learning based on common vulnerability scoring system. CMES - Computer Modeling in Engineering and Sciences **141**(2), 1551–1574 (2024). https://doi.org/10.32604/cmes.2024.052375
81. Kim, M., Wang, J., Moore, K., Goel, D., Wang, D., Mohsin, A., Ibrahim, A., Doss, R., Camtepe, S., Janicke, H.: CyberAlly: Leveraging LLMs and knowledge graphs to empower cyber defenders. In: Companion Proceedings of the ACM on Web Conference 2025, pp. 2851–2854. ACM, Sydney NSW Australia (2025). https://doi.org/10.1145/3701716.3715171
82. Kirkland, M.J., Steiner, S., Conte de Leon, D.: vWaterLabs: Design and characteristics of a virtual testbed for water-focused ICS cybersecurity education. J. Comput. Sci. Coll. **36**(8), 33–42 (2021)
83. Kombate, Y., Houngue, P., Ouya, S.: Securing MQTT: Unveiling vulnerabilities and innovating cyber range solutions. Procedia Computer Science **241**, 69–76 (2024). https://doi.org/10.1016/j.procs.2024.08.012
84. Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., Janicke, H.: The SAir-IIoT cyber testbed as a service: A novel cyber-twins architecture in IIoT-based smart airports. IEEE Trans. Intell. Transp. Syst. **24**(2), 2368–2381 (2023). https://doi.org/10.1109/TITS.2021.3106378
85. Kostage, K., Adepu, R., Monroe, J., Haughton, T., Mogollon, J., Poduvu, S., Palaniappan, K., Qu, C., Calyam, P., Mitra, R.: Federated learning-enabled network incident anomaly detection optimization for drone swarms. In: Proceedings of the 26th International Conference on Distributed Computing and Networking, ICDCN '25, pp. 104–114. Association for Computing Machinery, New York, NY, USA (2025). https://doi.org/10.1145/3700838.3700857
86. Krawiec, P., Janowski, R., Mongay Batalla, J., Andrukiewicz, E., Latoszek, W., Mavromoustakis, C.X.: On providing multi-level security assurance based on Common Criteria for O-RAN mobile network equipment. A test case: O-RAN Distributed Unit. Computers & Security **150**, 104271 (2025). https://doi.org/10.1016/j.cose.2024.104271
87. Kuchar, K., Blazek, P., Fujdiak, R.: From playground to battleground: Cyber range training for industrial cybersecurity education. In: Proceedings of the 2023 13th International Conference on Communication and Network Security, pp. 209–214. ACM (2023). https://doi.org/10.1145/3638782.3638814
88. Landauer, M., Mayer, K., Skopik, F., Wurzenberger, M., Kern, M.: Red team redemption: A structured comparison of open-source tools for adversary emulation (2024). https://arxiv.org/abs/2408.15645
89. Lazarov, W., Janek, S., Martinasek, Z., Fujdiak, R.: Event-based data collection and analysis in the cyber range environment. In: Proceedings of the 19th International Conference on Availability, Reliability and Security, pp. 1–8. ACM (2024). https://doi.org/10.1145/3664476.3670448
90. Lee, S.H., Choi, S.H., Jang, W., Shim, S., Kim, Y.J., Park, K.W.: Cyber-physical fuzzing framework for extracting butterfly effect in UAV systems. In: 2024 International Conference on AI x Data and Knowledge Engineering (AIxDKE), pp. 66–69 (2024). https://doi.org/10.1109/AIxDKE63520.2024.00018
91. Leitner, M., Frank, M., Hotwagner, W., Langner, G., Maurhart, O., Pahi, T., Reuter, L., Skopik, F., Smith, P., Warum, M.: AIT cyber range. In: Proceedings of the European Interdisciplinary Cybersecurity Conference, pp. 1–6. ACM (2020). https://doi.org/10.1145/3424954.3424959
92. Leonis, P., Ntouros, K., Mazilu, A.I., Brotsis, S., Kolokotronis, N.: SEAGuard: A blockchain-based security framework for IoT maritime transportation systems. In: 2024 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 421–426 (2024). https://doi.org/10.1109/CSR61664.2024.10679490
93. Lesueur, F., Noûs, C.: MI-LXC: A small-scale internet-like environment for network security teaching. In: Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, pp. 1–6. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3469181
94. Lieskovan, T., Hajny, J.: Security of smart grid networks in the cyber ranges. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1–8. ACM (2022). https://doi.org/10.1145/3538969.3543801
95. Lin, S., Xu, S., He, B., Liu, H., Kong, D., Chen, X., Zhang, D., Wu, C., Li, M., Liu, X., Wu, Y., Khan, M.K.: NDIF: A distributed framework for efficient in-network neural network inference. Computers & Security **157**, 104593 (2025). https://doi.org/10.1016/j.cose.2025.104593
96. Lin, W., Saifuddin, M.R., Chen, B.: The design and implementation of a cyber exercise on EPIC microgrid testbed. In: 2023 IEEE International Conference on Communications, Control, and

Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7 (2023). https://doi.org/10.1109/SmartGridComm57358.2023.10333919
97. Liu, C., Yan, W., Xu, F., Yang, W., Li, B.: User behavior simulation in ICS cyber ranges. In: 2022 19th Annual International Conference on Privacy, Security & Trust (PST), pp. 1–5 (2022). https://doi.org/10.1109/PST55820.2022.9851980
98. Lo, C., Win, T.Y., Rezaeifar, Z., Khan, Z., Legg, P.: Digital twins of cyber physical systems in smart manufacturing for threat simulation and detection with deep learning for time series classification. In: 2024 29th International Conference on Automation and Computing (ICAC), pp. 1–6 (2024). https://doi.org/10.1109/ICAC61394.2024.10718749
99. Longo, G., Orlich, A., Musante, S., Merlo, A., Russo, E.: MaCySTe: A virtual testbed for maritime cybersecurity. SoftwareX **23**, 101426 (2023). https://doi.org/10.1016/j.softx.2023.101426
100. Low, X., Yang, D., Yang, D.: Design and implementation of industrial control cyber range system. In: 2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 166–170 (2022). https://doi.org/10.1109/CyberC55534.2022.00034
101. Machaka, V., Figueroa-Lorenzo, S., Arrizabalaga, S., Elduayen-Echave, B., Hernantes, J.: Assessing the impact of Modbus/TCP protocol attacks on critical infrastructure: WWTP case study. Comput. Electr. Eng. **126**, 110485 (2025). https://doi.org/10.1016/j.compeleceng.2025.110485
102. Machaka, V., Figueroa-Lorenzo, S., Arrizabalaga, S., Hernantes, J.: Comparative analysis of the standalone and Hybrid SDN solutions for early detection of network channel attacks in Industrial Control Systems: A WWTP case study. Internet of Things **28**, 101413 (2024). https://doi.org/10.1016/j.iot.2024.101413
103. Maggi, F., Balduzzi, M., Vosseler, R., Rösler, M., Quadrini, W., Tavola, G., Pogliani, M., Quarta, D., Zanero, S.: Smart factory security: A case study on a modular smart manufacturing system. Procedia Computer Science **180**, 666–675 (2021). https://doi.org/10.1016/j.procs.2021.01.289
104. Mahmoud, R.V., Kidmose, E., Turkmen, A., Pilawka, O., Pedersen, J.M.: DefAtt - architecture of virtual cyber labs for research and education. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–7 (2021). https://doi.org/10.1109/CyberSA52016.2021.9478236
105. Makrakis, G.M., Roberson, D., Kolias, C., Cook, D.: Evaluation of SDN security measures in the context of IEC 62443–3-3. Int. J. Crit. Infrastruct. Prot. **47**, 100716 (2024). https://doi.org/10.1016/j.ijcip.2024.100716
106. Mashima, D., Roomi, M.M., Ng, B., Kalberczyk, Z., Suhail Hussain, S., Chang, E.C.: Towards automated generation of smart grid cyber range for cybersecurity experiments and training. In: 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-s), pp. 49–55 (2023). https://doi.org/10.1109/DSN-S58398.2023.00024
107. Mezaal, A.A., Zaghir, S.H., E.M.Abbas, Hashim, D.J., Almusawi, M., Sabah, M., Sabr, A.R.H.: Automated IOT security testbed: Design and implementation insights. In: 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), pp. 561–567 (2024). https://doi.org/10.1109/ICICAT62666.2024.10923460
108. Mishchenko, D., Oleinikova, I., Erdődi, L., Pokhrel, B.R.: Multidomain cyber-physical testbed for power system vulnerability assessment. IEEE access: practical innovations, open solutions **12**, 38135–38149 (2024). https://doi.org/10.1109/ACCESS.2024.3375401
109. Mohamed, H., Koroniotis, N., Schiliro, F., Moustafa, N.: IoT-CAD: A comprehensive digital forensics dataset for AI-based cyberattack attribution detection methods in IoT environments. Ad Hoc Netw. **174**, 103840 (2025). https://doi.org/10.1016/j.adhoc.2025.103840
110. Moradi, F., Abbaspour Asadollah, S., Pourvatan, B., Moezkarimi, Z., Sirjani, M.: CRYSTAL framework: Cybersecurity assurance for cyber-physical systems. Journal of Logical and Algebraic Methods in Programming **139**, 100965 (2024). https://doi.org/10.1016/j.jlamp.2024.100965
111. Moustafa, N.: A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustain. Cities Soc. **72**, 102994 (2021). https://doi.org/10.1016/j.scs.2021.102994
112. Murthy, A.K., Parthasarathi, R., Vetriselvi, V.: Security testbed for next generation mobile networks. In: 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), pp. 122–129 (2020). https://doi.org/10.1109/ISEA-ISAP49340.2020.235010
113. Mushi, M., Liu, Y., Sreenivasa, S., Ozdemir, O., Guvenc, I., Sichitiu, M., Dutta, R., Gyurek, R.: Open RAN testbeds with controlled air mobility. Comput. Commun. **228**, 107955 (2024). https://doi.org/10.1016/j.comcom.2024.107955
114. Musleh, A.S., Ahmed, J., Ahmed, N., Xu, H., Chen, G., Hu, J., Jha, S.: Development of a collaborative hybrid cyber-physical testbed for analysing cybersecurity issues of DER systems. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–6 (2023). https://doi.org/10.1109/SmartGridComm57358.2023.10333908
115. Musleh, A.S., Ahmed, J., Ahmed, N., Xu, H., Chen, G., Kerr, S., Jha, S.: Experimental cybersecurity evaluation of distributed solar inverters: Vulnerabilities and impacts on the australian grid. IEEE Transactions on Smart Grid **15**(5), 5139–5150 (2024). https://doi.org/10.1109/TSG.2024.3393439
116. Mustafa, H.M., Bariya, M., Sajan, K.S., Chhokra, A., Srivastava, A., Dubey, A., von Meier, A., Biswas, G.: RT-METER: A real-time, multi-layer cyber-power testbed for resiliency analysis. In: Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES '21, pp. 1–7. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3470481.3472708
117. Nakata, R., Otsuka, A.: CyExec*: A high-performance container-based cyber range with scenario randomization. IEEE access: practical innovations, open solutions **9**, 109095–109114 (2021). https://doi.org/10.1109/ACCESS.2021.3101245
118. National Initiative for Cybersecurity Education (NICE): Cyber ranges. One Pager, (2018)
119. Neema, H., Koutsoukos, X., Potteiger, B., Tang, C., Stouffer, K.: Simulation testbed for railway infrastructure security and resilience evaluation. In: Proceedings of the 7th Symposium on Hot Topics in the Science of Security, HotSoS '20, pp. 1–8. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3384217.3385623
120. Nelson, C., Shoshitaishvili, Y.: DOJO: Applied cybersecurity education in the browser. In: Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, SIGCSE 2024, pp. 930–936. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3626252.3630836
121. Nguyen, H.P.T., Hasegawa, K., Fukushima, K., Beuran, R.: PenGym: Realistic training environment for reinforcement learning pentesting agents. Computers & Security **148**, 104140 (2025). https://doi.org/10.1016/j.cose.2024.104140
122. Nguyen, T.T., Hooshyar, H., Kadavil, R.: A real-time cyber-physical simulation testbed for cybersecurity assessment of power systems. In: 2023 IEEE Industry Applications Society Annual Meeting (IAS), pp. 1–5 (2023). https://doi.org/10.1109/IAS54024.2023.10406799

123. Nguyen, T.T., Kadavil, R., Hooshyar, H.: A real-time cyber-physical simulation testbed for cybersecurity assessment of large-scale power systems. IEEE Trans. Ind. Appl. **60**(6), 8329–8340 (2024). https://doi.org/10.1109/TIA.2024.3457877
124. Oden Choi, J., Guttman, R., Kisow, M., Rosé, C., Nichols, W., Winyard, J., Li, B., Branstetter, L., Herckis, L.: Bridging the community college cybersecurity classroom and workplace with the CyberSim lab. In: Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1, pp. 875–881. ACM, Pittsburgh PA USA (2025). https://doi.org/10.1145/3641554.3701834
125. Oh, S.K., Stickney, N., Hawthorne, D., Matthews, S.J.: Teaching web-attacks on a raspberry pi cyber range. In: Proceedings of the 21st Annual Conference on Information Technology Education, pp. 324–329. ACM (2020). https://doi.org/10.1145/3368308.3415364
126. Ong, T.C., Premkumar, B., Guo, H.: Cyber range revolution: Transforming the future of cybersecurity training. In: 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 1–6 (2023). https://doi.org/10.1109/SOLI60636.2023.10425741
127. ÖZÇELİK, İ., İSKEFİYELİ, M., Balta, M., Ovaz Akpinar, K., Toker, F.S.: CENTER energy: A secure testbed infrastructure proposal for electricity power grid. In: 2021 International Conference on Information Security and Cryptology (ISCTURKEY), pp. 149–154 (2021). https://doi.org/10.1109/ISCTURKEY53027.2021.9654352
128. Palumickas, M., Yamin, M.M., Katt, B., Lal, C.: Evaluating ASCERT: Generative AI for cyber-range scenario generation. Int. J. Inf. Secur. **25**(1), 8 (2025). https://doi.org/10.1007/s10207-025-01179-w
129. Parada, R., Vilajosana, X., Alfayoumi, S., Serra, J., Font-Bach, O., Dini, P.: An open testbed for O-RAN experimentation with AI-enabled control and monitoring. Internet of Things **33**, 101729 (2025). https://doi.org/10.1016/j.iot.2025.101729
130. Park, G., Kim, J., Choi, J., Kim, J.: CryptoGuard: Lightweight hybrid detection and response to host-based cryptojackers in linux cloud environments. In: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, pp. 1617–1631. ACM, Hanoi Vietnam (2025). https://doi.org/10.1145/3708821.3736186
131. Potteiger, B., Cai, F., Dubey, A., Koutsoukos, X., Zhang, Z.: Security in mixed time and event triggered cyber-physical systems using moving target defense. In: 2020 IEEE 23rd International Symposium on Real-Time Distributed Computing (ISORC), pp. 89–97 (2020). https://doi.org/10.1109/ISORC49007.2020.00022
132. Praharaj, L., Gupta, D., Gupta, M.: A lightweight edge-CNN-transformer model for detecting coordinated cyber and digital twin attacks in cooperative smart farming. In: 2024 IEEE International Conference on Big Data (BigData), pp. 6346–6355 (2024). https://doi.org/10.1109/BigData62323.2024.10825128
133. Praharaj, L., Gupta, D., Gupta, M.: Efficient federated transfer learning-based network anomaly detection for cooperative smart farming infrastructure. Smart Agricultural Technology **10**, 100727 (2025). https://doi.org/10.1016/j.atech.2024.100727
134. Predescu, A.V., Stelkens-Kobsch, T.H.: Aviation Security Lab: A testbed for security testing of current and future aviation technologies. In: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), pp. 1–5 (2022). https://doi.org/10.1109/DASC55683.2022.9925750
135. Purves, T., Kyriakopoulos, K.G., Jenkins, S., Phillips, I., Dudman, T.: Causally aware reinforcement learning agents for autonomous cyber defence. Knowl.-Based Syst. **304**, 112521 (2024). https://doi.org/10.1016/j.knosys.2024.112521
136. Puys, M., Thevenon, P.H., Mocanu, S.: Hardware-in-the-loop labs for SCADA cybersecurity awareness and training. In: Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, pp. 1–10. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3469185
137. Qian, Y., Xie, H., Zhong, J., Chen, C., Bie, Z.: Resource allocation for hybrid quantum-classical communication systems in multiapplication-enabled power grids. IEEE Trans. Industr. Inf. **21**(1), 267–276 (2025). https://doi.org/10.1109/TII.2024.3452197
138. Qin, W.: Design and implementation of a cyber rang with emulated network security devices. In: 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT), pp. 1526–1531 (2023). https://doi.org/10.1109/ICCECT57938.2023.10141361
139. Rafy, M.F., Boateng, E.O., Krishnan, V.V.G., Srivastava, A.K.: Cyber-resilient IoT-based battery energy storage systems in power distribution system. IEEE Trans. Ind. Appl. **61**(3), 4566–4577 (2025). https://doi.org/10.1109/TIA.2025.3549413
140. Raj, A., Das, S., Vardhan, H., Neema, H., Chhokra, A., Balasubramanian, D.: Autonomous cybersecurity testbed for operational technology networks. In: Proceedings of the 7th Workshop on Design Automation for CPS and IoT, DESTION '25, pp. 1–6. Association for Computing Machinery, New York, NY, USA (2025). https://doi.org/10.1145/3722573.3727830
141. Rajkumar, K., shalinie, S.M.: Semi-supervised deep-ELM for DDoS attack detection and mitigation using the OptimalLink model in IoT networks. Computers & Security **152**, 104323 (2025). https://doi.org/10.1016/j.cose.2025.104323
142. Ramirez-Martinez, E.D., Pérez-Díaz, J.A., Yungaicela-Naula, N.M.: P4-Assisted Slowloris DDoS attack detection in IoT environments by using ML and DL. Comput. Netw. **267**, 111364 (2025). https://doi.org/10.1016/j.comnet.2025.111364
143. Ravikumar, G., Hyder, B., Govindarasu, M.: Efficient modelling of IEC-61850 logical nodes in IEDs for scalability in CPS security testbed. In: 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1–5 (2020). https://doi.org/10.1109/TD39804.2020.9299665
144. Ravikumar, G., Hyder, B., Govindarasu, M.: Next-generation CPS testbed-based grid exercise - synthetic grid, attack, and defense modelling. In: 2020 Resilience Week (RWS), pp. 92–98 (2020). https://doi.org/10.1109/RWS50334.2020.9241284
145. Rebecchi, F., Pastor, A., Mozo, A., Lombardo, C., Bruschi, R., Aliferis, I., Doriguzzi-Corin, R., Gouvas, P., Alvarez Romero, A., Angelogianni, A., Politis, I., Xenakis, C.: A digital twin for the 5G era: The SPIDER cyber range. In: 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 567–572 (2022). https://doi.org/10.1109/WoWMoM54355.2022.00088
146. Reghunath, R., Sayed, M.A., Sarieddine, K., Atallah, R., Jafarigiv, D., Kassouf, M., Assi, C., Ghafouri, M.: A real-time monitoring architecture for enhanced cybersecurity in the EV ecosystem. In: IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society, pp. 1–6 (2024). https://doi.org/10.1109/IECON55916.2024.10905899
147. Rigó, E., Árvai, P., Póser, V.: Cybersecurity and autonomous driving: Experiments with LiDAR sensor spoofing. In: 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), pp. 1–5 (2024). https://doi.org/10.1109/CIEES62939.2024.10811376
148. Roomi, M.M., Hwee, I.L.K., Mashima, D.: On design and implementation of real-time, high-fidelity virtual power system for smart grid cyber range. In: 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7 (2023). https://doi.org/10.1109/SmartGridComm57358.2023.10333893

149. Rouquette, R., Beau, S., Yamin, M.M., Mohib, U., Katt, B.: Automatic and realistic traffic generation in a cyber range. In: 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 352–358 (2023). https://doi.org/10.1109/FiCloud58648.2023.00058
150. Russo, E., Costa, G., Armando, A.: Building next generation cyber ranges with CRACK. Computers & Security **95**, 101837 (2020). https://doi.org/10.1016/j.cose.2020.101837
151. Russo, E., Ribaudo, M., Orlich, A., Longo, G., Armando, A.: Cyber range and cyber defense exercises: Gamification meets university students. In: Proceedings of the 2nd International Workshop on Gamification in Software Development, Verification, and Validation, pp. 29–37. ACM (2023). https://doi.org/10.1145/3617553.3617888
152. Sadlek, L., Yamin, M.M., Čeleda, P., Katt, B.: Severity-based triage of cybersecurity incidents using kill chain attack graphs. Journal of Information Security and Applications **89**, 103956 (2025). https://doi.org/10.1016/j.jisa.2024.103956
153. Sahani, N., Liu, C.C.: Model-based detection of coordinated attacks (DCA) in distribution systems. IEEE Open Access Journal of Power and Energy **11**, 558–570 (2024). https://doi.org/10.1109/OAJPE.2024.3489477
154. Saito, T., Takahashi, S., Sato, J., Matsunoki, M., Kanmachi, T., Yamada, S., Yajima, K.: Development of cyber ranges for operational technology. In: 2023 8th International Conference on Business and Industrial Research (ICBIR), pp. 1031–1034 (2023). https://doi.org/10.1109/ICBIR57571.2023.10147612
155. Sarieddine, K., Sayed, M.A., Torabi, S., Atallah, R., Assi, C.: Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations. International Journal of Electrical Power & Energy Systems **156**, 109735 (2024). https://doi.org/10.1016/j.ijepes.2023.109735
156. Sarkar, S., Teo, Y.M., Chang, E.C.: A cybersecurity assessment framework for virtual operational technology in power system automation. Simul. Model. Pract. Theory **117**, 102453 (2022). https://doi.org/10.1016/j.simpat.2021.102453
157. Sarker, P.S., Venkataramanan, V., Cardenas, D.S., Srivastava, A., Hahn, A., Miller, B.: Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5. In: 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, pp. 1–6 (2020). https://doi.org/10.1109/MSCPES49613.2020.9133689
158. Schmidt, H., Sutterfield, G., Farnell, C.: Addressing cybersecurity data and workforce scarcity with TROY: Testbed for resilient operational sYstems. In: 2024 IEEE Design Methodologies Conference (DMC), pp. 1–8 (2024). https://doi.org/10.1109/DMC62632.2024.10812169
159. Shahrouz, J.K., Analoui, M.: Privacy-aware revocation in VANETs with a Blockchain using accumulator. Vehicular Communications **53**, 100918 (2025). https://doi.org/10.1016/j.vehcom.2025.100918
160. Shandilya, S.K., Upadhyay, S., Kumar, A., Nagar, A.K.: AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. Futur. Gener. Comput. Syst. **127**, 297–308 (2022). https://doi.org/10.1016/j.future.2021.09.018
161. Shangting, M., Quan, P.: Industrial cyber range based on QEMU-IOL. In: 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), pp. 671–674 (2021). https://doi.org/10.1109/ICPECA51329.2021.9362692
162. Sharifi, A.Z., Vanijja, V., Pal, D., Anantasabkit, W.: CyberIoT: An initial conceptualization of a web-based cyber range for IoT. In: 2021 International Conference on Computational Performance Evaluation (ComPE), pp. 091–096 (2021). https://doi.org/10.1109/ComPE53109.2021.9752401
163. Sharma, G., Malley, D.J., Parle, D., Akowua, K., Padgaonkar, N.: Analysis and study of intelligent testbed for safeguarding nuclear and defense industry from AI-enabled cyberattacks. In: 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), vol. 2, pp. 1–6 (2024). https://doi.org/10.1109/IATMSI60426.2024.10502505
164. Sharma, G., Sherif, E., He, M., Boiten, E.: Analysis of cyber-attacks for modern digital railway system using cyber range. In: 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), pp. 1–6 (2022). https://doi.org/10.1109/IATMSI56455.2022.10119321
165. Shitole, A.B., Kandasamy, N.K., Liew, L.S., Sim, L., Bui, A.K.: Real-time digital twin of residential energy storage system for cyber-security study. In: 2021 IEEE 2nd International Conference on Smart Technologies for Power, Energy and Control (STPEC), pp. 1–6 (2021). https://doi.org/10.1109/STPEC52385.2021.9718616
166. Silva, M., Pinto, D., Vitorino, J., Gonçalves, J., Maia, E., Praça, I.: GeNIS: A modular dataset for network intrusion detection and classification. Data Brief **60**, 111487 (2025). https://doi.org/10.1016/j.dib.2025.111487
167. Singapore University of Technology and Design (SUTD): iTrust Testbeds: SWaT, WADI, and EPIC. https://www.sutd.edu.sg/itrust/itrust-labs/testbeds/ (2025). Accessed: 2025-08-01
168. Sipola, T., Kokkonen, T., Puura, M., Riuttanen, K.E., Pitkäniemi, K., Juutilainen, E., Kontio, T.: Digital Twin of Food Supply Chain for Cyber Exercises. Appl. Sci. **13**(12), 7138 (2023). https://doi.org/10.3390/app13127138
169. Song, J., Wang, C., Saudrais, C., Swanson, M.K., Greaney, E.A., Moon, Y.B.: Cyber-manufacturing system testbed development: Adversarial insider manipulation. Procedia CIRP **93**, 180–185 (2020). https://doi.org/10.1016/j.procir.2020.03.007
170. Srivastava, A., Zhao, J., Moore, K., Anagnostou, E.: Development of cyber-physical security simulation testbed in RTDS using modbus communication. In: 2024 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5 (2024). https://doi.org/10.1109/PESGM51994.2024.10689146
171. Sun, N., Wang, W., Liu, K., Li, D., Lü, J.: Hybrid framework for security evaluation in Internet of Vehicles. Computers & Security **153**, 104398 (2025). https://doi.org/10.1016/j.cose.2025.104398
172. Surapaneni, P., Bojjagani, S., Khan, M.K.: VESecure: Verifiable authentication and efficient key exchange for secure intelligent transport systems deployment. Vehicular Communications **49**, 100822 (2024). https://doi.org/10.1016/j.vehcom.2024.100822
173. Sutterfield, G., Schmidt, H., Farnell, C.: Real-time simulation and workforce development with TROY: Testbed for resilient operational systems. In: 2024 IEEE Design Methodologies Conference (DMC), pp. 1–7 (2024). https://doi.org/10.1109/DMC62632.2024.10812136
174. Syed, A., Nour, B., Pourzandi, M., Assi, C., Debbabi, M.: Comprehensive advanced persistent threats dataset. IEEE Networking Letters **7**(2), 150–154 (2025). https://doi.org/10.1109/LNET.2025.3551989
175. Tadese, Y.B., Shrestha, R., Dasari, B.K., Mohammadpour, M., Souto, L., Chamana, M., Adeyanju, O., Bayne, S.: Hybrid CNN-LSTM detection of cyber-attacks on MPPT controllers in PV systems. In: 2025 IEEE Texas Power and Energy Conference (TPEC), pp. 1–6 (2025). https://doi.org/10.1109/TPEC63981.2025.10906863
176. Tân, S.G., Liu, I.H., Li, J.S.: Threat analysis of cyber security exercise for reservoir testbed based on attack tree. In: 2022 Tenth International Symposium on Computing and Networking Workshops (CANDARW), pp. 375–379 (2022). https://doi.org/10.1109/CANDARW57323.2022.00023

177. Tan, Y., Liu, J., Li, Y., Wang, J.: Deep learning based proactive anomaly detection for 5G core control plane network function interactions. IEEE Transactions on Cognitive Communications and Networking pp. 1–1 (2025). https://doi.org/10.1109/TCCN.2025.3539660
178. Tarman, T., Rollins, T., Swiler, L., Cruz, J., Vugrin, E., Huang, H., Sahu, A., Wlazlo, P., Goulart, A., Davis, K.: Comparing reproduced cyber experimentation studies across different emulation testbeds. In: Proceedings of the 14th Cyber Security Experimentation and Test Workshop, CSET '21, pp. 63–71. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3474718.3474725
179. Terashima, T., Nakayama, M., Yokoyama, T., Koide, H.: KAKOI: A new tool to make simple and secure build cyber ranges using public cloud. In: 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), pp. 398–404 (2021). https://doi.org/10.1109/CANDARW53999.2021.00073
180. Thiyagarajan, K., Hammad, I.: Anomaly detection in air-gapped industrial control systems of nuclear power plants. In: 2024 Cyber Awareness and Research Symposium (CARS), pp. 1–6 (2024). https://doi.org/10.1109/CARS61786.2024.10778886
181. Thorpe, J., Swiler, L.P., Hanson, S., Cruz, G., Tarman, T., Rollins, T., Debusschere, B.J.: Verification of cyber emulation experiments through virtual machine and host metrics. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, CSET '22, pp. 71–80. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3546096.3546115
182. Torquato, M., Jesus, B., Silva, F.A., Cerqueira, E.: Empirical observation of execution throttling as MQTT broker defense against memory denial of service attacks. In: Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing, LADC '24, pp. 184–187. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3697090.3699870
183. Torquato, M., Maciel, P., Vieira, M.: Evaluation of time-based virtual machine migration as moving target defense against host-based attacks. J. Syst. Softw. **219**, 112222 (2025). https://doi.org/10.1016/j.jss.2024.112222
184. Trungadi, F., Fabiano, M., Aloisio, D., Brunaccini, G., Sergi, F., Merlino, G., Longo, F.: Securing Modbus in legacy industrial control systems: A decentralized approach using proxies, Post-Quantum Cryptography and Self-Sovereign Identity. Journal of Information Security and Applications **94**, 104199 (2025). https://doi.org/10.1016/j.jisa.2025.104199
185. Tse, A., Vattam, S., Ercolani, V., Stetson, D., Zurko, M.E.: A testbed for operations in the information environment. In: Proceedings of the 17th Cyber Security Experimentation and Test Workshop, CSET '24, pp. 83–90. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3675741.3675751
186. Tung, Y.C., Liou, E.C., Hu, P.C., Yu, C.H.: VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration. Computers & Security **157**, 104566 (2025). https://doi.org/10.1016/j.cose.2025.104566
187. Uçtu, G., Alkan, M., Doğru, İA., Dörterler, M.: A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls. Futur. Gener. Comput. Syst. **124**, 56–67 (2021). https://doi.org/10.1016/j.future.2021.05.013
188. Uetz, R., Hemminghaus, C., Hackländer, L., Schlipper, P., Henze, M.: Reproducible and adaptable log data generation for sound cybersecurity experiments. In: Proceedings of the 37th Annual Computer Security Applications Conference, ACSAC '21, pp. 690–705. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3485832.3488020
189. Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., Bellekens, X.: A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors **20**(24), 7148 (2020). https://doi.org/10.3390/s20247148
190. Umrani, M.I., Butler, B., O'Driscoll, A., Davy, S.: False data injection attacks on unmanned aerial vehicles used for package delivery. In: 2024 Cyber Research Conference - Ireland (Cyber-RCI), pp. 1–4 (2024). https://doi.org/10.1109/Cyber-RCI60769.2024.10939197
191. Vashishtha, L.K., Chatterjee, K.: Strengthening cybersecurity: TestCloudIDS dataset and SparkShield algorithm for robust threat detection. Computers & Security **151**, 104308 (2025). https://doi.org/10.1016/j.cose.2024.104308
192. Vasilakis, M., Karampidis, K., Tampouratzis, M., Malamos, A., Panagiotakis, S., Papadourakis, G.: Enhancing industry 4.0 cybersecurity training through cyber range platform. In: 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE), pp. 1–6 (2024). https://doi.org/10.1109/EEITE61750.2024.10654399
193. Vekaria, K.B., Calyam, P., Wang, S., Payyavula, R., Rockey, M., Ahmed, N.: Cyber range for research-inspired learning of "attack defense by pretense" principle and practice. IEEE Trans. Learn. Technol. **14**(3), 322–337 (2021). https://doi.org/10.1109/TLT.2021.3091904
194. Wagner, E., Bader, L., Wolsing, K., Serror, M.: Sherlock: A dataset for process-aware intrusion detection research on power grid networks: Dataset paper. In: Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy, pp. 419–424. ACM, Pittsburgh PA USA (2024). https://doi.org/10.1145/3714393.3726006
195. Wake, P., Black, S., Young, J.: Optimising IT security research via a low cost, instantly available, cloud based cyber range. In: 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, pp. 1–8 (2024). https://doi.org/10.1109/ICECET61485.2024.10698747
196. Wali, S., Farrukh, Y.A., Khan, I., Hamilton, J.A.: Covert penetrations: Analyzing and defending SCADA systems from stealth and Hijacking attacks. Computers & Security **156**, 104449 (2025). https://doi.org/10.1016/j.cose.2025.104449
197. Wan, Z., Cho, J.H., Zhu, M., Anwar, A., Kamhoua, C., Singh, M.: Optimizing effectiveness and defense of drone surveillance missions via honey drones. ACM Trans. Internet Technol. **24**(4), 22:1–22:26 (2024). https://doi.org/10.1145/3701233
198. Wang, L., Wei, Z., Guo, W.: Multi-agent deep reinforcement learning-based key generation for graph layer security. ACM Trans. Priv. Secur. **28**(2), 18:1–18:18 (2025). https://doi.org/10.1145/3711900
199. Wang, Z., Qi, D., Mei, J., Li, Z., Wan, K., Zhang, J.: Real-time controller hardware-in-the-loop co-simulation testbed for cooperative control strategy for cyber-physical power system. Global Energy Interconnection **4**(2), 214–224 (2021). https://doi.org/10.1016/j.gloei.2021.05.004
200. Wehbe, N., Alameddine, H.A., Pourzandi, M., Assi, C.: Empowering 5G SBA security: Time series transformer for HTTP/2 anomaly detection. Computers & Security **148**, 104114 (2025). https://doi.org/10.1016/j.cose.2024.104114
201. Wei, A., Bierbrauer, D., Nack, E., Pavlik, J., Bastian, N.: Offline reinforcement learning for autonomous cyber defense agents. In: Proceedings of the Winter Simulation Conference, WSC '24, pp. 1978–1989. IEEE Press, Orlando, Florida, USA (2025)
202. Weisman, M.J., Kott, A., Ellis, J.E., Murphy, B.J., Parker, T.W., Smith, S., Vandekerckhove, J.: Quantitative measurement of cyber resilience: Modeling and experimentation. ACM Trans. Cyber-Phys. Syst. **9**(1), 1:1–1:25 (2025). https://doi.org/10.1145/3703159

203. Wen, S.F., Yamin, M.M., Katt, B.: Ontology-Based Scenario Modeling for Cyber Security Exercise. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 249–258 (2021). https://doi.org/10.1109/EuroSPW54576.2021.00032
204. Wen, Z., Pacherkar, H.S., Yan, G.: VET5G: A virtual end-to-end testbed for 5G network security experimentation. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, CSET '22, pp. 19–29. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3546096.3546111
205. Wolsing, K., Saillard, A., Bauer, J., Wagner, E., van Sloun, C., Fink, I.B., Schmidt, M., Wehrle, K., Henze, M.: Network attacks against marine radar systems: A taxonomy, simulation environment, and dataset. In: 2022 IEEE 47th Conference on Local Computer Networks (LCN), pp. 114–122 (2022). https://doi.org/10.1109/LCN53696.2022.9843801
206. Yamin, M.M., Katt, B.: Modeling and executing cyber security exercise scenarios in cyber ranges. Computers & Security **116**, 102635 (2022). https://doi.org/10.1016/j.cose.2022.102635
207. Yamin, M.M., Katt, B.: Use of cyber attack and defense agents in cyber ranges: A case study. Computers & Security **122**, 102892 (2022). https://doi.org/10.1016/j.cose.2022.102892
208. Yamin, M.M., Katt, B., Gkioulos, V.: Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security **88**, 101636 (2020). https://doi.org/10.1016/j.cose.2019.101636
209. Yamin, M.M., Katt, B., Yamin, S., Ullah, M., Imran, A.S.: Large Language Models as a Cyber Range. In: 2026 7th International Conference on Advancements in Computational Sciences (ICACS), pp. 1–6 (2026). https://doi.org/10.1109/ICACS69208.2026.11433152
210. Yang, B., Guo, L., Ye, J.: Real-time simulation of electric vehicle powertrain: Hardware-in-the-loop (HIL) testbed for cyber-physical security. In: 2020 IEEE Transportation Electrification Conference & Expo (ITEC), pp. 63–68 (2020). https://doi.org/10.1109/ITEC48692.2020.9161525
211. Yeo, A.K.T., Garbelini, M.E., Chattopadhyay, S., Zhou, J.: VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench. Vehicular Communications **43**, 100649 (2023). https://doi.org/10.1016/j.vehcom.2023.100649
212. Zacharis, A., Patsakis, C.: AiCEF: An AI-assisted Cyber Exercise Content Generation Framework Using Named Entity Recognition (2022). https://doi.org/10.48550/arXiv.2211.10806
213. Zakharov, A.A., Khanbekov, S.I., Zakharova, I.G., Korenev, D.A.: Management of the cyber range functionality based on the analysis of the digital footprint of students. In: 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE), pp. 920–924 (2023). https://doi.org/10.1109/APEIE59731.2023.10347585
214. Zhang, C., Shao, W., Wang, X., Cao, Y., Alhamadah, A.H.J., Lin, Y.Z., Satam, P., Watkins, L.: Explainable autonomic cybersecurity system for smart power grid. In: 2024 IEEE Conference on Communications and Network Security (CNS), pp. 1–6 (2024). https://doi.org/10.1109/CNS62487.2024.10735649
215. Zhang, C., Zeng, L., Zhu, J., Wang, L., Shafiq, M., Du, X.: RED-scenario: A resource-efficient deployment framework for scenarios through dependency package management. IEEE Communications Magazine pp. 1–7 (2025). https://doi.org/10.1109/MCOM.002.2400601
216. Zhang, Y., Liu, Z., Jia, C., Zhu, Y., Miao, C.: An online defense against object-based LiDAR attacks in autonomous driving. In: Proceedings of the 22nd ACM Conference on Embedded Networked Sensor Systems, pp. 380–393. ACM, Hangzhou China (2024). https://doi.org/10.1145/3666025.3699345
217. Zhou, H., Li, M., Sun, Y., Yun, L., Tian, Z.: Digital twin-based cyber range for industrial internet of things. IEEE Consumer Electronics Magazine **12**(6), 66–77 (2023). https://doi.org/10.1109/MCE.2022.3203202
218. Zola, F., Echeberria, X., Petisco, J., Vakakis, N., Voulgaridis, A., Votis, K.: KINAITICS: Enhancing cybersecurity education using AI-based tools and gamification. In: Proceedings of the 2024 16th International Conference on Education Technology and Computers, pp. 138–147. ACM, Porto Vlaams-Brabant Portugal (2024). https://doi.org/10.1145/3702163.3702183

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