CYBERTASTE STUDIE

Cyber Range Technology Stack and Simulations for Training and Evaluation

Klaus Mayer
Max Landauer
Florian Skopik
Markus Wurzenberger

Kontakt
Markus Wurzenberger
markus.wurzenberger@ait.ac.at
AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Wien

Das Projekt „CyberTASTE – Cyber Range Technology Stack and Simulations for Training and Evaluation“ wird gefördert bzw. finanziert im Rahmen des Sicherheitsforschungsförderprogramm KIRAS durch das Bundesministerium für Finanzen (BMF) und von der Österreichischen Forschungsförderungsgesellschaft (FFG) abgewickelt.

11.9.2026

CyberTASTE: Cyber Range Technology Stack and Simulations for Training and Evaluation

Klaus Mayer, Max Landauer, Florian Skopik, and Markus Wurzenberger

AIT Austrian Institute of Technology, Vienna, Austria
E-Mail: firstname.lastname@ait.ac.at

Abstrakt

Die CyberTASTE Studie untersucht, wie Cyber Ranges (CRs) und Testbeds (TBs) in der Praxis umgesetzt werden, mit besonderem Fokus auf die Technologien, die zur Realisierung von CR/TB-Use Cases und -Funktionen eingesetzt werden. Aufbauend auf einer systematischen Literaturrecherche im Zeitraum 2020 bis August 2025 umfasst die Studie 199 Publikationen und konsolidiert die extrahierten Anwendungsbereiche, Zwecke, Use Cases, Infrastrukturtypen und dokumentierten Technologien in einer strukturierten Datengrundlage zur Analyse. Das Repository identifiziert 650 einzelne Technologien und ordnet diese einer hierarchischen Struktur aus 10 Technologiedomänen und 81 Technologie-Subdomänen zu, um trotz heterogener Terminologie und unterschiedlicher architektonischer Darstellungen einen konsistenten Vergleich zwischen den Publikationen zu ermöglichen. Die Analyse weist auf eine funktionale Trennung in den berichteten Implementierungen hin: TBs werden häufiger für experimentell orientierte Use Cases berichtet, während CRs häufiger für Training, Übungen und Ausbildung eingesetzt werden. Über die Anwendungsbereiche hinweg zeigen die Daten konzentrierte Profile sowie explizite Lücken in bestimmten Domänen-/Anwendungsbereichskombinationen, für die keine Technologien berichtet werden, wobei zeitliche Trends auf eine zunehmende Diversifizierung der berichteten Use Cases in den Jahren 2024–2025 hindeuten. Basierend auf diesen Mustern und den diskutierten Herausforderungen einer uneinheitlichen Terminologie und Kategorisierung empfiehlt die vorliegende Arbeit eine systematischere Berichterstattung von Technologien und Funktionsimplementierungen sowie die Verwendung einer gemeinsamen Terminologie mit expliziten Zuordnungen zu Referenzarchitekturen oder Taxonomien.

Erklärungen

Nutzung von AI: Für die Übersetzung einzelner Textpassagen, die auch in der Publikation "Mayer K., Landauer M., Skopik F., Wurzenberger M. (2026): Engineering Cyber Ranges and Security Testbeds: A Survey of Technologies, Use Cases, and Research Trends. International Journal of Information Security, forthcoming, Springer. (accepted)"veröffentlicht wurden, wurden KI-gestützte Übersetzungswerkzeuge (Large Language Models) verwendet. Die inhaltliche Verantwortung sowie die fachliche Prüfung und Freigabe aller Inhalte erfolgten durch die Autor*innen.

Funding: Diese Studie wurde durch die Österreichische Forschungsförderungsgesellschaft (FFG) im Rahmen des Projekts CyberTASTE (Förderungsnummer FO999905294) gefördert.

Inhaltsverzeichnis

Abkürzungen

2FA Two-Factor Authentication

ACM Association for Computing Machinery

AERPAW Aerial Experimentation and Research Platform for Advanced Wireless

AI Artificial Intelligence

AIT Austrian Institute of Technology

API Application Programming Interface

APT Advanced Persistent Threat

ARP Address Resolution Protocol

AWS Amazon Web Services

BSSID Basic Service Set Identifier

BTrDB Berkeley Tree Database

CIS Center for Internet Security

CNN Convolutional Neural Network

CPS Cyber-Physical Systems

CR Cyber Range

CRX Cyber Range Exercise

CSV Comma-Separated Values

CTF Capture the Flag

CyRIS Cyber Range Instantiation System

DDoS Distributed Denial-of-Service

DMZ Demilitarised Zone

DNP3 Distributed Network Protocol 3

DNS Domain Name System

DoS Denial-of-Service

DVWA Damn Vulnerable Web Application

EC2 Elastic Compute Cloud

ECSO European Cyber Security Organisation

EDR Endpoint Detection and Response

ELK Elasticsearch, Logstash, and Kibana

EV Electric Vehicle

FDI False-Data Injection

5G Fifth-Generation Mobile Network

FTP File Transfer Protocol

gNB gNodeB

GOOSE Generic Object Oriented Substation Event

GUI Graphical User Interface

HiL Hardware-in-the-Loop

HMI Human–Machine Interface

HTTP Hypertext Transfer Protocol

IaC Infrastructure as Code

IAM Identity and Access Management

ICS Industrial Control Systems

ICT Information and Communication Technology

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

IEEE Institute of Electrical and Electronics Engineers

IIoT Industrial Internet of Things

IoT Internet of Things

IPFIX IP Flow Information Export

IPFS InterPlanetary File System

IPS Intrusion Prevention System

IT Information Technology

JSON JavaScript Object Notation

KVM Kernel-based Virtual Machine

LAMP Linux, Apache, MySQL, and PHP

LLM Large Language Model

LMS Learning Management System

LTS Long-Term Support

MFA Multi-Factor Authentication

ML Machine Learning

MQTT Message Queuing Telemetry Transport

NIDS Network Intrusion Detection System

NIST National Institute of Standards and Technology

NMEA National Marine Electronics Association

NoSQL Not Only SQL

ns-3 Network Simulator 3

NSF National Science Foundation

OAuth Open Authorization

OPC Open Platform Communications

OPC UA OPC Unified Architecture

OpenJDK Open Java Development Kit

O-RAN Open Radio Access Network

OT Operational Technology

OTP One-Time Passcode

PDU Protocol Data Unit

PLC Programmable Logic Controller

RAN Radio Access Network

RIC RAN Intelligent Controller

RTDS Real-Time Digital Simulator

S3 Simple Storage Service

SCADA Supervisory Control and Data Acquisition

SCMS Security Credential Management System

SCP Secure Copy Protocol

SDL Scenario Description Language

SDN Software-Defined Networking

SIEM Security Information and Event Management

6G Sixth-Generation Mobile Network

SNMP Simple Network Management Protocol

SOAR Security Orchestration, Automation, and Response

SQL Structured Query Language

SSH Secure Shell

TB Testbed

TCP Transmission Control Protocol

TDMS Technical Data Management Streaming

TTP Tactics, Techniques, and Procedures

UAV Unmanned Aerial Vehicle

UDP User Datagram Protocol

UE User Equipment

UI User Interface

URL Uniform Resource Locator

VANET Vehicular Ad Hoc Network

VM Virtual Machine

VNC Virtual Network Computing

VPN Virtual Private Network

WWTP Wastewater Treatment Plant

YAML YAML Ain't Markup Language

1. Einleitung

Cyber Ranges (CRs) und Testbeds (TBs) sind in der modernen Cybersicherheit von zentraler Bedeutung. Sie bieten realistische Plattformen für die Ausbildung von Fachkräften im Bereich Informations- und Kommunikationstechnologien, was angesichts der steigenden Anzahl an Cyberangriffen und -bedrohungen zunehmend wichtiger wird. Die Bedeutung und Relevanz von CRs und TBs in der Cybersicherheit nimmt stetig zu und wurde in den letzten Jahren wiederholt in verwandten Übersichtsarbeiten hervorgehoben [190]. Darüber hinaus bestätigt auch ihr vielseitiger wissenschaftlicher Einsatz für Forschung, Experimente, und Tests [91], sowie ihre Verbreitung in der Industrie die Relevanz dieser Technologien [71]. Laut [71] besteht weiterhin Bedarf an klaren Richtlinien, die Konzeption, Entwicklung, Evaluierung und Betrieb von CRs abdecken. Während sich mehrere Studien mit zentralen Aspekten von CRs befassen, wiederholen oder paraphrasieren diese häufig primär etablierte Standards und interpretieren diese in manchen Fällen sogar uneinheitlich, anstatt zusätzliche neuartige Erkenntnisse und konkrete, eindeutige Handlungsempfehlungen für die Gestaltung und den Betrieb einer CR bereitzustellen. Wie auch in [190] festgestellt wird, bestehen trotz ihrer wachsenden Relevanz weiterhin Forschungslücken, und eine umfassende, konsolidierte Analyse als zentrale Referenz für die Community fehlt nach wie vor.

Eine zentrale Herausforderung bei der Konzeption und dem Betrieb einer CR oder eines TB ist die große Anzahl potenziell geeigneter Technologien und die daraus resultierende Komplexität der Technologieauswahl. Im Rahmen dieser Literaturstudie wurden beispielsweise 650 einzelne Technologien identifiziert, die zur Entwicklung von CRs, TBs und unterschiedlichen Use Cases eingesetzt werden können. Dies führte zu folgenden Forschungsfragen:

- **RQ1:** Welche Use Cases und Anwendungsbereiche für CRs und TBs werden in der Literatur berichtet?
- **RQ2:** Welche Technologien und Technologiegruppen werden zur Umsetzung spezifischer CR-/TB-Funktionen eingesetzt?
- **RQ3:** Welche Trends und bemerkenswerten Muster lassen sich in der Forschung und Entwicklung von CRs und TBs beobachten (z. B. hinsichtlich Zwecke, Anwendungsbereiche und Technologien)?

Ein wesentlicher Teil bestehender Übersichtsarbeiten befasst sich mit allgemeinen Funktionen und der Architektur von CRs und TBs. Mehrere Ansätze schlagen Taxonomien und Modelle zur Kategorisierung von Funktionen, Use Cases und architektonischen Darstellungen vor. Nach bestem Wissen der Autor*innen ist jedoch [209] die einzige Übersichtsarbeit, die sich primär auf die digitalen Bausteine einer CR oder eines TB konzentriert, insbesondere auf die zu deren Umsetzung eingesetzten Technologien. Ziel der CyberTASTE Studie ist es daher, einen Überblick über aktuelle Technologien zu geben und die Auswahl von Technologien zur Umsetzung von Use Cases und Funktionen in CRs und TBs zu erleichtern. Als Ausgangspunkt dient [209], welche eine Liste von Technologien bereitstellt, die in CRs und TBs eingesetzt wurden, einschließlich des dokumentierten Jahres und Anwendungsbereichs. Die Ergebnisse dieser Untersuchung sind in [107] veröffentlicht, angenommen zur Publikation im *International Journal of Information Security* (Springer). Zusammenfassend liefert diese Arbeit folgende Beiträge:

- Einen Überblick über CRs und TBs, einschließlich ihrer *Anwendungsbereiche* und Zwecke.
- Eine Liste von in CRs und TBs eingesetzten Technologien, zusammen mit deren beabsichtigtem Einsatzzweck.
- Die Identifikation von Lücken und bemerkenswerten Mustern hinsichtlich Technologien, CRs und TBs.

- Einen praxisorientierten Leitfaden zur Technologieauswahl für CRs.

Der Aufbau dieser Arbeit gliedert sich wie folgt: Kapitel 2 gibt einen Überblick über verwandte Arbeiten und führt die in dieser Arbeit verwendeten Definitionen von CR und TB ein. Kapitel 3 beschreibt die Methodik der systematischen Literaturrecherche. Kapitel 4 präsentiert die Ergebnisse hinsichtlich Zwecken, Use Cases und eingesetzten Technologien. Kapitel 5 diskutiert Herausforderungen, Muster und Trends und beantwortet die Forschungsfragen. Kapitel 6 übersetzt die gewonnenen Erkenntnisse in einen praxisorientierten Leitfaden zur Technologieauswahl für CRs. Abschließend skizziert Kapitel 7 Richtungen für zukünftige Forschung, bevor Kapitel 8 die Arbeit zusammenfasst.

2. Hintergrund und verwandte Arbeiten

Dieser Kapitel fasst relevante Publikationen zusammen, die sich mit Funktionalitäten, Fähigkeiten und architektonischen Aspekten vonCRs und TBs befassen. Die daraus extrahierten zentralen Beiträge umfassen Klassifikationen und Taxonomien von CR-/TB-Merkmalen, vorgeschlagene Referenzarchitekturen, Frameworks oder konzeptuelle Modelle sowie Evaluierungen bestehender CRs/TBs, einschließlich Diskussionen zu *Zwecken*, *Anwendungsbereichen* und unterstützenden Technologien.

Ukwandu et al. [190] bieten einen systematischen Überblick über CRs und Sicherheits-TBs, mit Fokus darauf, wie diese Plattformen für das Cybersicherheitstraining eingesetzt werden und wie sie sich angesichts zunehmender Automatisierung von Angriffen sowie der Konvergenz von Information Technology (IT) und Operational Technology (OT) weiterentwickeln könnten. Sie untersuchen Literatur hauptsächlich aus dem Zeitraum 2015 bis 2020 und analysieren CR/TB-Plattformen nach *Anwendungsbereichen*, Bereitstellungsmodell, Experimentierungsansatz (Simulation, Emulation, hybrid), Teamstrukturen und zugrunde liegenden Technologien wie Virtualisierung, Containerisierung und physischer Hardware. Basierend auf dieser Erkenntnissen vergleicht der Beitrag typische Szenariomerkmale und Angriffstypen in CRs und TBs. Die Arbeit stellt fest, dass TBs häufig mit kritischen Infrastrukturen und OT-Umgebungen verknüpft sind, während CRs häufiger in der Information and Communication Technology (ICT)-orientierten Aus- und Weiterbildung eingesetzt werden. Ein zentraler Beitrag des Artikels ist der Vorschlag zweier eigenständiger Taxonomien. Eine Taxonomie fokussiert sich auf CRs, die andere auf TBs. Diese Taxonomien ordnen Aspekte wie Verwaltung und Monitoring, Szenariodesign (einschließlich pädagogischer Mechanismen und Gamification), Angriffstypen sowie Wiederherstellungsfunktionen. Die Taxonomie für TBs umfasst zusätzlich Dimensionen für Modellierung und Ausführung. Die Autor*innen diskutieren zudem die von CRs und TBs unterstützten Trainingsmethoden. Sie argumentieren, dass die Abgrenzung zwischen diesen beiden Plattformtypen zunehmend unschärfer wird. Der Artikel hebt aufkommende Trends hervor, darunter die Entwicklung stärker konfigurierbarer und echtzeitfähiger Umgebungen sowie breitere Anwendungskontexte wie cyberphysische Systeme und Industrie 4.0. Auch potenzielle Erweiterungen, wie die Integration von Augmented Reality, werden untersucht.

Chouliaras et al. [38] untersuchen Cyber Ranges und Sicherheits-Testbeds, die für Cybersicherheitsausbildung, Training, Übungen und Forschung eingesetzt werden, und setzen dabei an einem in der Praxis bestehenden Defizit an: Viele Studien erwähnen Plattformen zwar, beschreiben jedoch nur begrenzte Details zu Architektur, Topologie und konkreten Implementierungswerkzeugen. Die Autor*innen stellen zunächst eine Reihe von Cyber Ranges/Testbeds aus der Literatur zusammen und charakterisieren diese (z. B. nach Betreiber, Zielen, Sektor, Umgebungstyp und Infrastruktur) und führen anschließend strukturierte Interviews mit technischen Leiter*innen von zehn ausgewählten Plattformen durch, um andernfalls dokumentierte Design- und Betriebsdetails zu erfassen, darunter Szenarienerstellung und -bereitstellung, Übungsverwaltung sowie die eingesetzten Technologien. Basierend auf den Interviewdaten synthetisiert der Beitrag eine tool- und komponentenorientierte Sicht auf aktuelle Cyber-Range-Implementierungen. Die Arbeit berichtet über gängige Nutzungsmuster (primär Training, häufig kombiniert mit Forschung/Übungen), thematische Schwerpunkte von CRs wie Wettbewerbe (zum Beispiel Capture the Flag (CTF)) und SCADA/ICS sowie typische Herausforderungsfelder (z. B. Websicherheit, Forensik, Exploitation und Malware-Analyse). Die Studie dokumentiert zudem häufig eingesetzte Technologien über die verschiedenen Plattformen hinweg, darunter Cloud- und Infrastrukturlösungen (z. B. OpenStack und AWS), Virtualisierungs- und Containeransätze (z. B. Hypervisoren und Docker), IaC-Werkzeuge (z. B. Ansible, Vagrant und Packer), Formate zur Szenariobeschreibung (überwiegend JSON und YAML) sowie Monitoring-/Sicherheitskomponenten (z. B. OSSIM, Nagios, Snort

und Suricata), und diskutiert Datensatzgenerierung, Fernzugriff/Föderation sowie einen Trend hin zu Digital-twin-ähnlichen Umgebungen.

Kampourakis et al. [71] schlagen eine feingranulare Referenzarchitektur für Cyber Ranges vor, motiviert durch die IT/OT-Konvergenz in Industrie 5.0 sowie den Bedarf an realistischen, standardkonformen Umgebungen für die Cybersicherheitsvorsorge. Sie argumentieren, dass bestehende Arbeiten Design, Entwicklung, Evaluierung und Betrieb von Cyber Ranges nicht gemeinsam vollständig und aktuell adressieren. Um diese Lücke zu schließen, leiten die Autor*innen ein abstraktes Modell aus relevanten Richtlinien und Standards ab, verfeinern es anhand häufig berichteter Cyber-Range-Funktionalitäten und -Merkmale und führen eine Bewertungsformel ein, um abzuschätzen, wie stark eine gegebene Cyber Range dem Stand der Technik entspricht. Der zentrale Beitrag ist eine Architekturbeschreibung, die gemäß ISO/IEC/IEEE 42010 strukturiert ist. Sie ist in eine strukturelle, eine funktionale und eine informationelle Sicht gegliedert. In der strukturellen Sicht kann die adressierte Zielumgebung entweder ein dediziertes Testbed oder ein Digital Twin sein. Diese Umgebung ist in Infrastruktur-, Virtualisierungs- und Orchestrierungsschichten eingebettet. Der Beitrag untersucht typische Virtualisierungsoptionen, darunter öffentliche oder private Cloud-Lösungen, virtuelle Maschinen und Container. Zudem werden Plattformen wie AWS, OpenStack, VMware und Docker referenziert. Darüber hinaus behandelt der Beitrag Orchestrierungsmethoden, einschließlich des Einsatzes von Controllern, Infrastructure as Code (IaC) und APIs. Die Bewertungsmethode wird anhand von Beispielevaluierungen mittels kriterienbasierter Bewertung und visuellem Vergleich demonstriert, und die Autor*innen positionieren die Arbeit als Grundlage für eine verbesserte Vereinheitlichung und Standardisierung, wobei eine Proof-of-Concept-Implementierung als zukünftige Arbeit geplant ist.

Insgesamt bieten die oben genannten Arbeiten einen systematischen Überblick über CRs, mit primärem Fokus auf Architekturen, Taxonomien sowie die strukturellen und funktionalen Konzepte, die dem CR-Design zugrunde liegen. Yamin et al. [209] präsentieren eine systematische Literaturübersicht zu nicht klassifizierten CRs und Sicherheits-TBs als Umgebungen zur Durchführung von Cybersicherheits-Trainingsszenarien, die sowohl kompetenzorientiertes Training für Sicherheitsfachkräfte als auch breiter angelegtes, sensibilisierungsorientiertes Training abdecken. Die Studie folgt einem strukturierten Review-Protokoll, das von drei Forschenden umgesetzt wurde. Dabei werden wichtige wissenschaftliche Datenbanken (Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE) Xplore, ScienceDirect, Springer Link und Wiley) im Publikationszeitraum 2002 bis 2019 mithilfe von Schlagwörtern zu CR, TB und Übungen durchsucht. Basierend auf den extrahierten Belegen entwickeln die Autor*innen eine Taxonomie für CR-Systeme und evaluieren die Literatur mit Schwerpunkt auf Architektur und Szenarien, wobei auch Fähigkeiten, Rollen, Werkzeuge und Bewertungskriterien berücksichtigt werden. Ein wesentlicher Beitrag ist das Kapitel „Tools“, das die konkreten Tools und Mechanismen, die über die untersuchten Plattformen hinweg berichtet werden, organisiert und vergleicht, darunter Emulation, Simulation, Hardware, Verwaltung, Monitoring, Traffic-Generierung, Generierung von Nutzer*innenverhalten, Scoring, Szenariodefinition und Sicherheitstests, mit detaillierten Tabellen für jede Kategorie. Der Beitrag hebt häufig genannte Tools hervor, etwa im Bereich Monitoring (z. B. Tcpdump, IP Flow Information Export (IPFIX), Wireshark), Emulationswerkzeuge (z. B. VMware und Emulab) und Simulationswerkzeuge (z. B. Qualnet, Simulink, Network Simulator, Matlab), und diskutiert auch die Rolle physischer Komponenten (z. B. Cisco-basierte Geräte und Programmable Logic Controller (PLC)-Geräte) in mehreren TBs. Abschließend synthetisieren die Autor*innen die untersuchten Architekturen zu einer einheitlichen funktionalen Architektur (z. B. Portal-, Verwaltungs-, Trainings-/Ausbildungs- und Testmodule) und diskutieren beobachtete Trends wie eine Verschiebung hin zu dynamischen Szenarien und zunehmende Automatisierung.

Die CyberTASTE Studie baut auf dieser Literaturübersicht auf, indem sie Publikationen ab 2020 untersucht und einen ähnlichen Schwerpunkt auf die in CRs und TBs eingesetzten Technologien

legt.

2.1. Definitionen

In der untersuchten Literatur werden mehrere, leicht unterschiedliche Definitionen von CRs und TBs verwendet. Basierend auf den erhobenen Daten erscheinen einige dieser Definitionen nicht mehr zutreffend. Ukwandu et al. [190] unterscheiden CRs und TBs beispielsweise dadurch, dass CRs überwiegend in IT-Umgebungen eingesetzt werden, während TBs in OT-Umgebungen bevorzugt werden. Die aktuelle Analyse legt nahe, dass diese Unterscheidung nicht mehr zutrifft, wie in Abschnitt 4.2 diskutiert wird. Darüber hinaus beschreiben Kampourakis et al. [71] TBs im Gegensatz zu CRs als Infrastrukturen, die typischerweise einem vordefinierten funktionalen Zweck dienen. In derselben Argumentationslinie beschreiben sie eine CR – ähnlich wie Yamin et al. [209] – als eine Umgebung, die solche TBs bereitstellt. Chouliaras et al. [38] weisen darauf hin, dass in der Literatur mehrere Definitionen von CRs existieren. Als pragmatischen Bezugspunkt übernehmen sie die Definition aus dem National Institute of Standards and Technology (NIST)-Einseiter [119] als „Erste unter Gleichen“. Diese Definition betont interaktive und simulierte Abbildungen der vernetzten Umgebung einer Organisation, die sowohl praxisnahen Kompetenzaufbau als auch Produktentwicklung und Sicherheitstests unterstützen. Die vorliegende Studie zeigt jedoch, dass CRs nicht auf rein simulierte Infrastrukturen beschränkt sind. Vielmehr können sie auch physische Komponenten integrieren, beispielsweise über Hardware-in-the-Loop (HiL)-Systeme, die reale Geräte mit simulierten Umgebungen verbinden. Basierend auf diesen Beobachtungen werden aktualisierte Definitionen von CRs und TBs vorgeschlagen, die eine technologiezentrierte Perspektive widerspiegeln und auf der im Rahmen dieser Studie erhobenen empirischen Evidenz beruhen.

Definition (Cyber Range)
Eine CR ist ein Technology Stack zur Konstruktion einer oder mehrerer isolierter virtueller oder hybrider Infrastrukturen für Zwecke wie Training, Ausbildung, Forschung, Tests und Experimente.

Definition (Testbed)
Ein TB ist eine isolierte Infrastrukturumgebung, die virtuell, physisch oder hybrid sein kann und für Training, Ausbildung, Forschung, Tests und Experimente konzipiert ist.

Verhältnis zwischen Cyber Ranges, Testbeds und Digital Twins
In der hier verwendeten Terminologie instanziiert eine CR eine oder mehrere *Zielinfrastrukturen*, die die Form von TBs und/oder Digital Twins annehmen können.

3. Methodik

Dieses Kapitel beschreibt den Ansatz zur Datenerhebung und systematischen Literaturrecherche. Zunächst wird die Suchstrategie skizziert, die zur Erstellung der ursprünglichen Literaturliste verwendet wurde. Anschließend werden die Kriterien beschrieben, die zur Filterung dieser ursprünglichen Liste angewendet wurden, um die Wissensbasis für diese Arbeit zu bilden. Abschließend wird erläutert, welche Datenpunkte aus den erfassten Artikeln extrahiert wurden.

3.1. Suchstrategie

Um einen umfassenden Überblick über die in CRs und TBs eingesetzten Technologien zu erhalten, wurden die Suchkriterien für die Literaturrecherche bewusst breit gefasst. Dies spiegelt sich im Suchanfrage wider. Obwohl der Fokus auf den eingesetzten Technologien liegt, wurden alle Artikel zu Security, CRs und TBs aus sämtlichen Anwendungsdomänen berücksichtigt. Um diesen breiten Umfang abzudecken, wurde ein Suchstring mit den Begriffen „Cyber Range(s)“, „Testbed(s)“, „Cybersecurity“, „Cyber Defense“ und „IT Security“ zusammengestellt. Der finale String wurde wie folgt formuliert:

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

Für die Literaturrecherche wurden folgende Suchmaschinen verwendet: Science Direct, ACM Digital Library und IEEE Xplore. Diese Arbeit baut auf dem Beitrag von [209] auf, der Publikationen bis Ende 2019 untersuchte. Der erste angewendete Filter war daher der Untersuchungszeitraum von 2020 bis August 2025. Die verbleibenden Publikationen wurden anschließend primär anhand von Einschlusskriterien und Abstrakts vorgefiltert. Dieser Prozess ergab 631 im Rahmen der systematischen Literaturrecherche identifizierte Publikationen, die anschließend gemäß Ein- und Ausschlusskriterien gefiltert wurden. Insgesamt wurden 199 Artikel in die Studie aufgenommen.
Einschlusskriterien:

- Die Publikation muss den Bereichen Security und Informatik zuzuordnen sein. Dies umfasst unter anderem Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA) und Cyber-Physical Systems (CPS).
- Die Publikation muss einen deutlichen Schwerpunkt auf CRs und/oder TBs legen oder einen erheblichen Teil ihres Inhalts diesen Themen widmen. Sie sollte eine angemessene technische Dokumentation der technologischen Komponenten, des Systemdesigns und der Implementierungsdetails bieten, anstatt rein konzeptuelle Diskussionen zu führen.
- Die Publikation muss in englischer Sprache verfasst sein.

Ausschlusskriterien:

- Sekundär- und Tertiärliteratur, etwa Übersichtsarbeiten, Reviews und ähnliche Publikationen, wurden ausgeschlossen.
- TBs aus anderen Domänen als der Informatik wurden ausgeschlossen.
- TBs mit Fokus auf die Sicherheit von Bauwerken sowie die Sicherheit/den Schutz von Personen wurden ausgeschlossen.
- TBs, die primär aus Hardware bestehen, wurden ausgeschlossen.

- Konferenzabstracts, Buchrezensionen, Konferenzinformationen, Extended Abstracts, Diskussionsbeiträge, Proposals, Editorials, Kurzrezensionen, Nachrichten und Kurzmitteilungen wurden ausgeschlossen.
- Publikationen, die nicht in elektronischer Form verfügbar waren, wurden ausgeschlossen.
- Bücher, technische Berichte, Vorlesungsskripte, Präsentationen, Rezensionen und Dissertationen/Abschlussarbeiten wurden ausgeschlossen. In diesen Fällen wurden, sofern verfügbar, die entsprechenden Konferenz- oder Zeitschriftenpublikationen herangezogen.
- Studien, die keine konkreten Technologien angeben oder die diskutierten Technologien unzureichend beschreiben, werden von der Übersicht ausgeschlossen.

3.2. Datenauswahl und Qualitätsbewertung

Dieser Abschnitt erläutert die Methodik und Strukturierung des Datenerhebungsprozesses genauer. Zudem werden die Qualitätskriterien beschrieben, die sowohl bei der Auswahl der Publikationen als auch bei der Extraktion der Technologiedaten angewendet wurden. Zur Beantwortung der Forschungsfragen wurden Informationen aus den Publikationen selbst sowie aus der darin beschriebenen Infrastruktur erhoben, namentlich CRs und TBs sowie den zugehörigen Technologien. Abbildung 1 bietet einen Überblick über die erhobenen Informationsobjekte und deren Struktur. Aufgrund des großen Umfangs werden Beispiele für konkrete Ausprägungen dieser Kategorien hier nicht beschrieben, sondern in Abschnitt 4 vorgestellt. Eine komprimierte Version der Datengrundlage findet sich zudem in Anhang A. Die blau hervorgehobenen Felder kennzeichnen die Bereiche, in denen aktiv Informationen erhoben wurden, während die nicht hervorgehobenen Felder zusätzliche, nicht kategorisierte Informationen enthalten. Die grau dargestellten Felder repräsentieren die Kategorienamen, die zur Klassifikation und Strukturierung der Technologien und Infrastrukturen entwickelt wurden. Diese Kategorien werden in diesem Abschnitt erläutert und im weiteren Verlauf dieser Arbeit durchgängig verwendet. Zur Entwicklung und Benennung der Kategorien wurden zunächst die relevanten Informationen aus jeder Publikation extrahiert und in einer konsolidierten Liste unter Beibehaltung der ursprünglichen Formulierung der Quelle erfasst. Anschließend wurden die extrahierten Einträge semantisch gruppiert, um Kategoriedefinitionen und -bezeichnungen abzuleiten. Diese Kategorien wurden daraufhin genutzt, um die Terminologie über die Publikationen hinweg zu harmonisieren und jeden Eintrag dem finalen, für die Analyse verwendeten Kategoriensatz zuzuordnen.

Qualitätskriterium auf Studienebene

Über die formalen Ein- und Ausschlusskriterien aus Abschnitt 3.1 hinaus wurde im Volltext-Review ein zusätzlicher Qualitätsschwellenwert auf Studienebene angewendet. Dabei wurde bewertet, ob die Publikationen ausreichende und eindeutige technische Details lieferten, um eine aussagekräftige Datenextraktion zu ermöglichen. Publikationen, in denen Technologien nur beiläufig erwähnt wurden, ohne deren Rolle in der CR oder dem TB zu beschreiben, wurden ausgeschlossen, selbst wenn sie die formalen Einschlusskriterien erfüllten. Dieses Kriterium adressiert die praktische Qualitätsdimension der Extrahierbarkeit von Daten, das heißt, ob ein Beitrag strukturierte und zuordenbare Belege zur Beantwortung der Forschungsfragen liefert.

In virtualisierten Infrastrukturen kommt eine Vielzahl unterschiedlicher Technologien zum Einsatz. Um Klarheit und analytischen Fokus zu wahren, wurden die Einträge in der Liste auf Technologien beschränkt, die direkt relevant für den Aufbau der CR oder des TB sowie für die Umsetzung der jeweiligen *Use Cases* sind. Die folgenden Absätze erläutern daher die Abgrenzungsentscheidungen und Einschränkungen, die bei der Erstellung der finalen Technologieliste angewendet wurden.

Implementierungsvoraussetzung
Technologien, die lediglich in verwandten Arbeiten erwähnt oder als potenzielle Optionen diskutiert, jedoch nicht tatsächlich implementiert wurden, wurden von dieser Analyse ausgeschlossen.

Relevanz für den CR-/TB-Zweck
Ebenso wurde allgegenwärtige Software oder Protokolle für allgemeine Zwecke, die nicht speziell für CRs oder deren *Use Cases* konzipiert sind, nicht aufgenommen. Dieser Ausschluss betrifft gängige Betriebssysteme wie Windows oder Linux, Standarddatenformate wie .txt oder .exe sowie weit verbreitete Protokolle wie Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP).

Hardware-Einschlusskriterium
Physische Geräte und Hardware wurden ebenfalls ausgeschlossen, sofern sie nicht für die Umsetzung des Szenarios essenziell und in der jeweiligen Publikation explizit beschrieben waren (z. B. ein Real-Time Digital Simulator (RTDS) im Industrial Control Systems (ICS)-Bereich).

Wiederverwendbarkeitskriterium
Individuelle Skripte und Ad-hoc-Programme wurden nicht aufgenommen. Die zu deren Erstellung verwendeten Entwicklungs-Frameworks und -Bibliotheken wurden hingegen berücksichtigt, da diese Komponenten wiederverwendbar und über Studien hinweg vergleichbar sind.

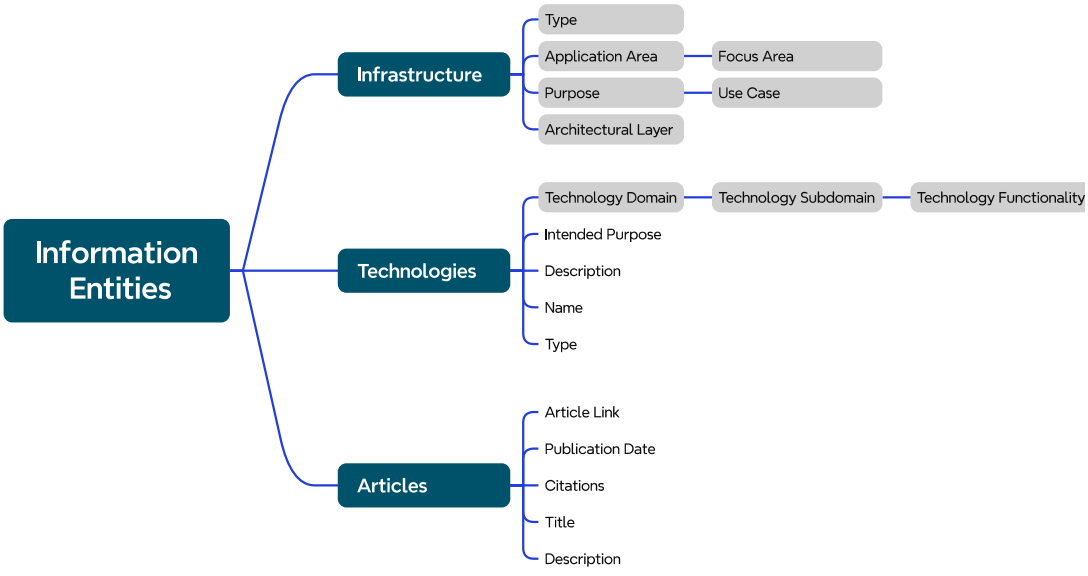


Abbildung 1: Strukturierter Überblick über die aus den Publikationen abgeleiteten Informationen und Kategorien.

3.2.1. Infrastruktur

Dieser Abschnitt beschreibt die Datenpunkte, die zur Charakterisierung der CR- oder TB-Infrastruktur erhoben wurden. Dazu zählen der Anwendungsbereich und die damit verbundenen Zwecke, der Architektur-Layer, in der eine Technologie verortet ist, sowie die Technologien selbst.

Anwendungsbereiche

Die *Anwendungsbereiche* repräsentieren die Umgebung, für die die CR oder das TB entwickelt wurde. Beispiele hierfür sind ICT und ICS. Zunächst wurden die Bezeichnungen genau so übernommen, wie sie in der jeweiligen Publikation beschrieben wurden. Anschließend wurden semantisch ähnliche Bezeichnungen harmonisiert und jene beibehalten, die als übergeordnete Kategorien aufgetreten sind und am häufigsten vorkamen, um Konsistenz über die Quellen hinweg zu gewährleisten. Obwohl CRs und TBs mehrere *Anwendungsbereiche* unterstützen können, konzentrieren sich die Publikationen typischerweise auf einen einzigen. Daher wurde in dieser Arbeit jede Publikation und die darin beschriebene Infrastruktur nur einem *Anwendungsbereich* zugeordnet. Für eine feingranularere Klassifikation unterteilten sind diese *Anwendungsbereiche* mit demselben Verfahren zusätzlich in *Fokusbereiche* unterteilt.

Zwecke

Die Studie von Yamin et al. zu CRs und Sicherheits-TBs [209] identifiziert *Testing*, *Education* und *Experiment* als CR-Zwecke. Die Autor*innen berichten, dass Testing-Szenarien im Zeitverlauf (bis 2019) zunehmend an Bedeutung gewannen. In einer 2021 durchgeführten Befragung von technischen Leiter*innen, die direkt in eine CR involviert waren, fragten Chouliaras et al. [38] nach den Zwecken von CRs und TBs und berichteten folgende Antworten: *Research*, *Training*, *Exercise*, *Education*, *Testing* und *Education Labs*. Die meisten Befragten nannten *Training* als primären Zweck. Der Beitrag von Katsantonis et al. zu einem CR-Design-Framework [76] unterscheidet drei Arten von CRs basierend auf Zielen und Absichten. *Educational* CRs werden für Ausbildung und Training eingesetzt und bieten eine organisierte Lernumgebung für praxisnahes Üben im Bereich Cybersicherheit. *Certification* CRs bewerten und zertifizieren die Cybersicherheitskenntnisse und -fähigkeiten der Teilnehmenden, häufig im Rahmen von Wettbewerben. *Test* CRs werden für Forschung und zum Testen von Cybersicherheitsprodukten (Technologien, Tools usw.) eingesetzt. Die Studie von Kampourakis et al. zu einer Referenzarchitektur [71] argumentiert ähnlich, dass *Education* und *Competence Building* zentrale Schwerpunkte der CR-Zwecke darstellen. Die Autor*innen gruppieren Zwecke in *Education*, *Research* und *Competence Building*. *Research* unterteilen sie weiter in *Testing* und *Experimentation*, *Competence Building* in *Training*, *Assessment* und *Classification*. Basierend auf den von uns analysierten Publikationen konsolidierten wurden die identifizierten *Use Cases* zu drei *Zweck*-Kategorien: *Research, Testing and Experimentation*, *Training and Exercises* und *Education*. Dieses Set an *Zwecken* steht im Einklang mit den oben beschriebenen Übersichtsarbeiten. Einzelne *Use Cases* verfeinern jeden *Zweck* weiter zu spezifischeren Kategorien und wurden aus dem Kontext jeder Publikation extrahiert und anschließend gruppiert. Mehrere der untersuchten Publikationen konzentrieren sich auf die Konstruktion und das Design von CRs oder TBs für bestimmte Ziele. Da die Technologieauswahl häufig Ziele wie ein kosteneffizientes CR-Design oder die Optimierung von Skalierbarkeit und Performance betrifft, wurde die Kategorie *System Architecture and Implementation* als zusätzlichen Filter für die Guideline zur Technologieauswahl eingeführt.

Architekturschichten

Die Literatur berichtet mehrere Varianten der strukturellen Organisation einer CR. Kampourakis et al. [71] beschreiben eigenständige *Zonen*, in denen die in Abschnitt 3.2.1 genannten Module

angesiedelt sind. Die *Target Infrastructure Zone* liegt innerhalb der *Core Infrastructure Zone* und bezeichnet die von der CR instanziierte Infrastruktur. Dabei kann es sich um ein TB oder einen Digital Twin handeln. Die *Underlying Infrastructure* bildet das Rückgrat der CR, umfasst Hardware, Software, Server und Netzwerktechnik und stellt die Infrastruktur dar, auf der die CR bereitgestellt wird. Ebenfalls innerhalb der *Core Infrastructure Zone* liegen die *Virtualization*- und *Orchestration*-Zonen. Hier werden Tools wie OpenStack, Docker oder VMware eingesetzt, um virtuelle Maschinen zu instanziieren, sowie Tools wie Ansible oder Terraform zur Orchestrierung der Systeme. Technologien dieser Art bilden die Computing-Plattform von CRs. Außerhalb der Core Infrastructure Zone stellt die *Learning Management and Support Zone* Services und Tools für Lehrende und Lernende bereit, ebenso wie Technologien zur Erstellung, Anpassung und Bereitstellung von Szenarien, Tactics, Techniques, and Procedures (TTPs) und zur Traffic-Generierung. Die *Monitoring and Management Zone* enthält Module zum Monitoring von Nutzenden und Szenarien, während die *Access Control Zone* Authentifizierungs- und Autorisierungsmodule umfasst. Laut Ukwandu et al. [190] bilden Emulation, Simulation, Virtualisierung und Containerisierung die Kerntechnologien einer CR. Darüber liegt die *Orchestration Layer*, die Infrastrukturtechnologien wie vSphere und Wisper umfasst. Die *CR Capabilities Layer* umfasst Funktionalitäten und Fähigkeiten, wie in Abschnitt 3.2.1 dargestellt, und die *Front-End Technologies Layer* stellt die Benutzeroberfläche der CR bereit. Um Technologien innerhalb architektonischer Zonen oder Schichten zu positionieren, wurden die Funktionalitäten in vier Layer (siehe Abbildung 2) gruppiert. Die Abbildung veranschaulicht nicht nur die Layer-Struktur, sondern hebt auch die am häufigsten genannten *Technologiedomänen* innerhalb jedes Layers hervor.

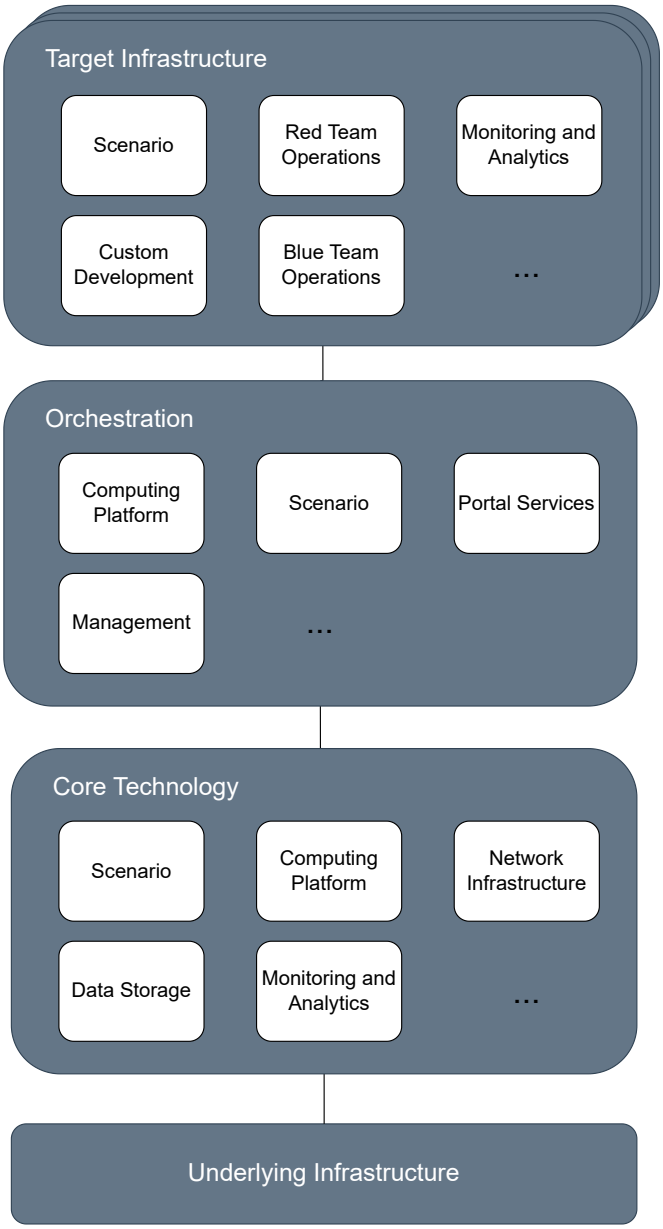


Abbildung 2: Architektur-Layer einer Cyber Range mit beispielhaften Funktionen je Layer.

Der Layer *Underlying Infrastructure* umfasst die Hardware, auf der die CR oder das TB bereitgestellt wird. Dies kann Server, Hardware von Cloud-Anbietern, verteilte Hosts, einen einzelnen Host oder andere geeignete Geräte einschließen. Dieser Layer wird der Vollständigkeit halber angeführt, liegt jedoch außerhalb des Fokus dieser Arbeit. Die *Core Technology Layer* umfasst primär Computing-Plattform-Technologien, die zur Instanziierung der Zielinfrastrukturen der CR eingesetzt werden. Typische Beispiele sind Cloud-Infrastruktur-Tools wie OpenStack, Amazon Web Services (AWS) oder Google Cloud, Virtualisierungsplattformen mit Typ-1- und Typ-2-Hypervisoren wie VMware vSphere oder VirtualBox sowie Containerisierungstechnologien wie Docker. Die *Orchestration Layer* umfasst Container-Orchestrierungs-Tools wie Kubernetes, Software- und Infrastructure-Provisioning- und Konfigurations-Tools wie Ansible und Terraform sowie Datenformate wie YAML Ain't Markup Language (YAML). Diese können als Sprachen zur

Szenariospezifikation und -beschreibung verwendet werden und unterstützen die automatisierte Instanziierung der Zielinfrastruktur. Der oberste Layer besteht aus einer oder mehreren *Target Infrastructures* und enthält alle Technologien und Funktionalitäten, die zur Umsetzung der jeweiligen *Use Cases* erforderlich sind.

Es ist wichtig anzumerken, dass Technologien und Funktionalitäten nicht in jeder CR eindeutig nur einem Layer zugeordnet werden können. Beispielsweise setzt die CR von Nelson et al. [121] QEMU, eine Virtualisierungstechnologie, innerhalb eines Docker-Containers ein. In diesem Szenario wird Docker der Core Technology Layer zugeordnet, während QEMU der Target Infrastructure Layer zugeordnet wird. Ein weiteres Beispiel sind Datenspeichertechnologien wie relationale Datenbanken. Diese finden sich in der Target Infrastructure Layer, wo sie als Trainingssysteme für Structured Query Language (SQL)-Injection Übungen in Red-Teaming Szenarien dienen, wie von Vasilakis et al. [193] beschrieben. Zudem präsentiert die Literatur integrierte CR-Lösungen und zugehörige Tools, die mehrere Layer abdecken. Diese können daher in mehr als einem Teil der Architektur verortet werden.

Technologien

Aus den untersuchten Publikationen wurden zudem die in CRs und TBs eingesetzten Technologien identifizierte und kategorisiert. Die ausgewählten Technologien bestimmen die Funktionalitäten und Fähigkeiten der CR oder des TB. Kampourakis et al. [71] gruppieren CR-Funktionalitäten in Module, darunter *Scoring & Reporting*, *Users & Scenario Monitoring*, *Data Collection & Analysis*, *Assets Monitoring*, *Scenario Development*, *Traffic Generation* und viele weitere. Yamin et al. [209] zerlegen die funktionale Architektur ähnlich in Module und Submodule. Beispiele hierfür sind *Management* (für CR, Szenario, Übung oder Test) und *Portal* (für Nutzende, Admin oder Client). Ukwandu et al. [190] und der European Cyber Security Organisation (ECSO)-Bericht *Understanding Cyber Ranges: From Hype to Reality* [57] bieten anschauliche Listen von Funktionalitäten und Fähigkeiten, die eine CR bieten kann. Dazu zählen Instructor-Tools, Internet-Services Simulation, Angriffssimulation, Kompetenzmanagement, Visualisierung, Reporting und Trainingsmethoden. Beide Quellen betonen, dass die Beispiele nicht vollständig sind und eine CR nicht alle aufgeführten Funktionen implementieren muss. In Anlehnung an die in diesen Publikationen verwendete Terminologie und basierend auf den identifizierten Technologien wurde eine hierarchische Taxonomie konstruiert, bestehend aus einer Kategorie *Technology Domain* mit 10 Einträgen und einer Kategorie *Technology Subdomain* mit 81 Einträgen, sowie einer Kategorie *Technology Functionality*, die den genauen *Zweck* jeder Technologie spezifiziert. Zusätzlich wurde der *Technologietyp* als eine der folgenden Ausprägungen analysiert: Tool, Datenformat, Framework, Library, OS, Plattform, Protokoll oder Technology Stack.

Artikel

Für jede Publikation fügten wurde der Liste neben Titel, Jahr und Link alle relevanten Felder hinzugefügt. Von den offiziellen Websites jeder Technologiewurde der Website-Link, der ursprünglich beabsichtigten Einsatzzweck sowie eine Kurzbeschreibung dokumentiert, da sich der Einsatzzweck innerhalb von CRs vom primären *Zweck* der Technologie unterscheiden kann. Für die CRs und TBs selbst wurden ebenfalls prägnante Beschreibungen aus den jeweiligen Publikationen extrahiert.

4. Ergebnisse

In diesem Kapitel werden zunächst die Ergebnisse der Literaturübersicht vorgestellt und anschließend, basierend auf den für CRs und TBs etablierten Kategorien und Strukturen, erläutert, wie unterschiedliche Funktionalitäten innerhalb der jeweiligen Domänen und *Use Cases* realisiert werden. Das Kapitel schließt mit einer Darstellung von Abhängigkeiten und Anforderungen über *Use Cases* hinweg sowie von Lücken in spezifischen Forschungsthemen.

4.1. Literaturübersicht

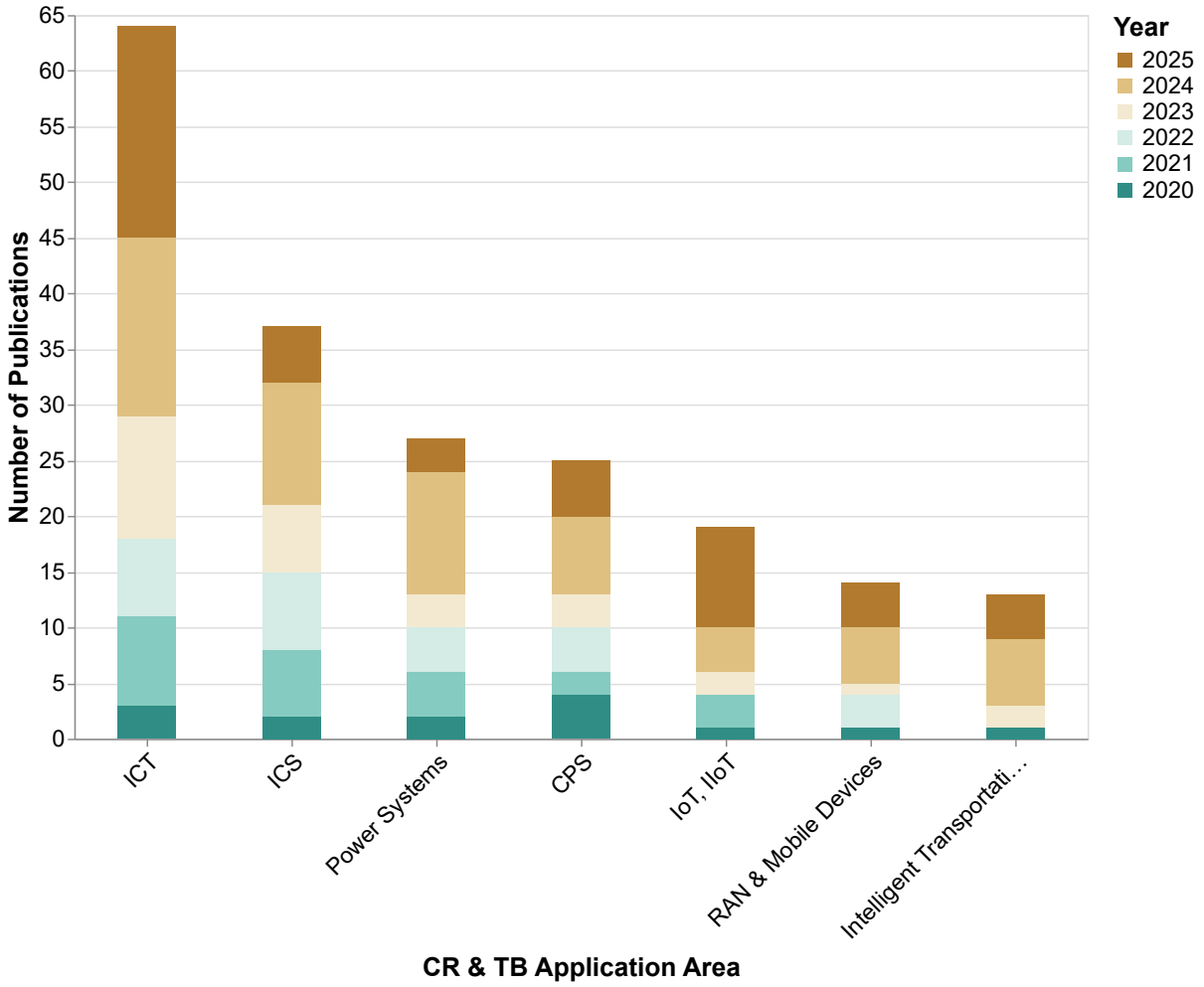


Abbildung 3: Publikationen je Anwendungsbereich.

Das gestapelte Balkendiagramm (Abbildung 3) fasst die Verteilung von 199 eindeutigen Publikationen zu CRs und TBs über die CR- und TB-*Anwendungsbereiche* für den Zeitraum 2020–2025 zusammen. Die Publikationsaktivität steigt insgesamt von 14 Beiträgen (2020) auf 28 (2023), gefolgt von einem ausgeprägten Höhepunkt im Jahr 2024 (60) und einem weiterhin hohen Volumen im Jahr 2025 (49). Über den gesamten Zeitraum hinweg dominiert ICT mit 64 Beiträgen (32,2 %), gefolgt von ICS (37; 18 %), Power Systems (27; 13 %) und CPS (25; 12 %). Kleinere, aber sichtbare Bereiche sind IoT/Industrial Internet of Things (IIoT) (19; 9,5 %), Radio Access Network (RAN) & Mobile Devices (14; 7,0 %) und Intelligent Transportation Systems (13; 6,5 %).

4.2. Zwecke und Use Cases von Cyber Ranges und Testbeds

Abbildung 4 visualisiert die Verteilung der identifizierten Publikationen über *Anwendungsbereiche*, *Zwecke* und Infrastrukturtypen von CRs und TBs mittels eines Sankey-Diagramms. Links sind die CR- und TB-Anwendungsbereiche aufgeführt (zum Beispiel ICT, ICS, CPS, IoT/IIoT, Power Systems, Intelligent Transportation Systems und RAN & Mobile Devices). In der Mitte werden die drei übergeordneten *Zweck*-Kategorien dargestellt, nämlich Education, Research, Testing and Experimentation sowie Training and Exercises. Rechts werden die Infrastrukturtypen (CR und TB) angezeigt. Die Breite der Verbindungen zwischen den Knoten ist proportional zur Anzahl der eindeutigen Publikationen, die mindestens einen *Use Case* für die jeweilige Kombination aus *Anwendungsbereich*, *Zweck* und Infrastrukturtyp beschreiben. Jede Publikation wird genau einem *Anwendungsbereich* und genau einem Infrastrukturtyp (entweder CR oder TB) zugeordnet, kann jedoch mehrere *Zwecke* adressieren. Folglich kann eine Publikation aus der ICT-Domäne in mehreren *Zweck*-Kategorien erscheinen, wird jedoch nie parallel mehreren Infrastrukturtypen zugeordnet. In der Analyse kann eine Publikation daher über die *Zweck*-Kategorien hinweg mehrfach gezählt werden, jedoch höchstens einmal pro Kombination aus *Anwendungsbereich*, *Zweck* und Infrastrukturtyp. Die Analyse zeigt, dass der *Zweck* Research, Testing and Experimentation (RTE) im *Anwendungsbereich* ICT am stärksten vertreten ist, mit insgesamt 41 Publikationen (18 mit CRs und 23 mit TBs). Im Gegensatz dazu werden die *Zwecke* Education sowie Training and Exercises in ICT überwiegend mittels CRs umgesetzt, wobei 14 von 15 Education-Publikationen und 21 von 22 trainingsbezogenen Publikationen auf CR-basierten Umgebungen beruhen. In ICS erstreckt sich RTE über 29 Publikationen (3 CR und 26 TB), während Training and Exercises in 13 Publikationen vertreten ist, die nahezu gleichmäßig auf CR (7) und TB (6) verteilt sind. Andere Domänen, darunter CPS, IoT/IIoT, Power Systems und Intelligent Transportation Systems, weisen eine starke Dominanz von TBs in RTE-Kontexten auf. In manchen Fällen (zum Beispiel Intelligent Transportation Systems) treten CRs überhaupt nicht auf. Insgesamt zeigt das Sankey-Diagramm, dass RTE über die meisten *Anwendungsbereiche* hinweg der vorherrschende *Zweck* ist, jedoch überwiegend mittels TBs realisiert wird. CRs werden insbesondere in ICT (und teilweise in ICS sowie RAN & Mobile Devices) für Training and Exercises sowie Bildungszwecke eingesetzt. In den folgenden Unterkapiteln werden für jeden der drei *Zwecke* die am häufigsten berichteten *Use Cases* vorgestellt, jeweils ergänzt durch konkrete Beispiele ihrer Umsetzung aus der analysierten Literatur.

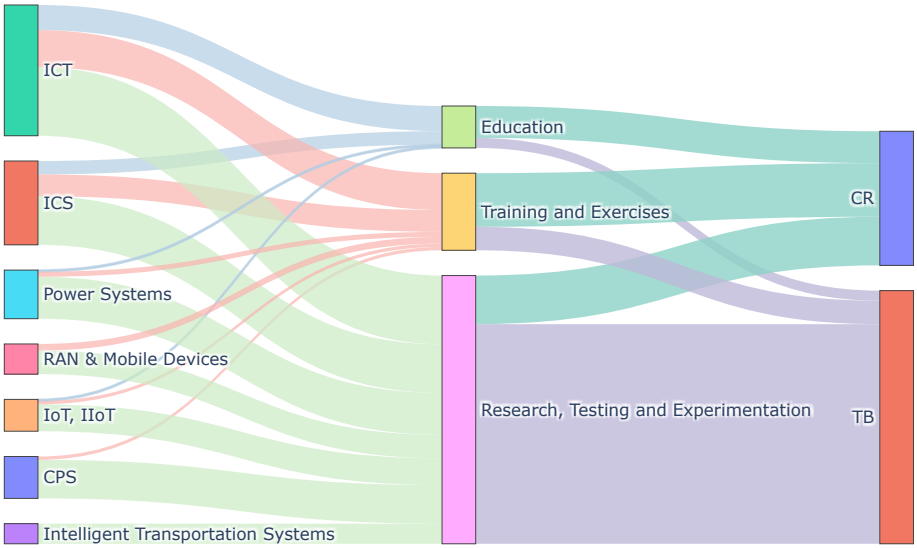


Abbildung 4: Verteilung der *Anwendungsbereiche* von Cyber Ranges und Testbeds über Zwecke und Infrastrukturtypen.

4.2.1. Research, Testing and Experimentation

Abbildung 5 fasst die zehn am häufigsten genannten *Use Cases* für den *Zweck* „Research, Testing and Experimentation“ über CRs (CR) und TBs (TB) hinweg zusammen. Da ein einzelner Artikel mehrere *Use Cases* beschreiben kann, zählen die Balken Use-Case-Nennungen und nicht eindeutige Publikationen. Der Datensatz umfasst insgesamt 305 Nennungen. Die zehn am häufigsten genannten *Use Cases* machen 171 Nennungen aus (56,1 %). Alle übrigen *Use Cases* werden jeweils weniger als fünfmal genannt und sind daher nicht in der Abbildung dargestellt. Zusammen machen sie 134 Nennungen aus (43,9 %). Über die Plattformtypen hinweg dominiert TB mit 257 Nennungen (84,3 %), gefolgt von CR mit 48 Nennungen (15,7 %). Unter den einzeln benannten *Use Cases* führt „Threat and Vulnerability Assessment“ mit 46 Nennungen, gefolgt von „Attack Impact Assessment“ (35) und „Dataset Generation“ (29). Die nächste Gruppe umfasst „Cyber Security Resilience Assessment“ (18) und „Mitigation Strategies“ (10). Weitere, seltener genannte *Use Cases* sind „Machine Learning (ML)-based Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)“ (9), „Anomaly Detection“ (8) und „Artificial Intelligence (AI)-based Anomaly Detection“ (6), wobei sowohl „Cyber Security Risk Assessment“ als auch „Traffic Generation“ die Top 10 mit jeweils 5 Nennungen abschließen. Insgesamt dominieren evaluationsorientierte Aktivitäten (Threat-/Vulnerability- und Impact-Assessments), ergänzt durch Dataset-Generierung und Resilience-Tests, während erkennungs- und ML-fokussierte *Use Cases* durchgängig, jedoch mit geringeren absoluten Häufigkeiten auftreten.

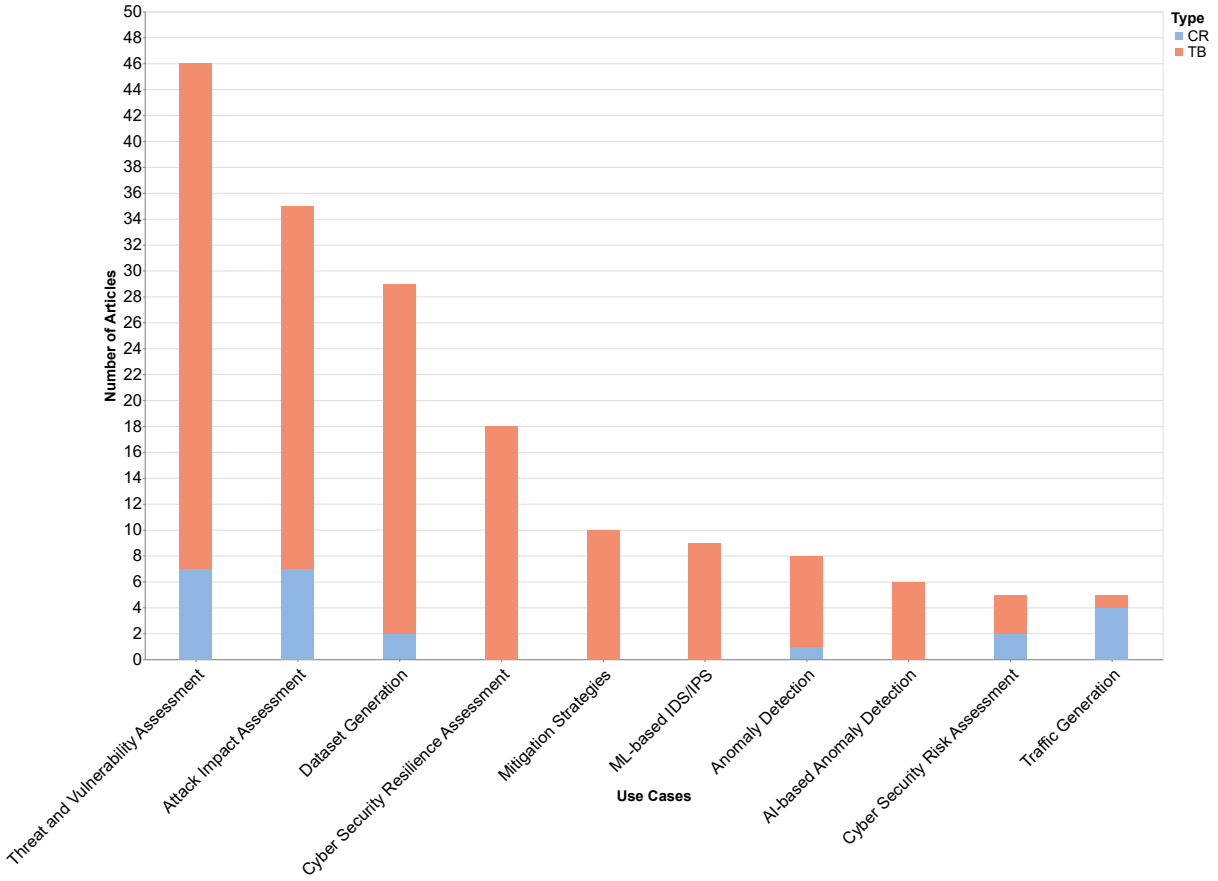


Abbildung 5: Top-10 Use Cases für den Zweck „Research, Testing and Experimentation“ über Cyber Ranges (CR) und Testbeds (TB) hinweg.

Threat and Vulnerability Assessment

Ein experimenteller Aufbau für Security-Tests von IoT- und Webanwendungen setzt eine Zielumgebung ein, die mithilfe von Tools wie Acunetix systematisch gescannt und untersucht wird. Dabei entstehen Traffic und Ergebnisse, die zur Bewertung von Schwachstellen und Fehlkonfigurationen im TB genutzt werden [116]. Ein Sicherheits-TB für Systeme der nächsten Generation integriert externe Threat-Intelligence-Feeds wie URLhaus in eine kontrollierte Umgebung und nutzt die gesammelten bösartigen Uniform Resource Locators (URLs), um malwarebezogene Inhalte abzurufen und zu analysieren. Dadurch wird bewertet, wie gut unterschiedliche Abwehrmechanismen diese Bedrohungen erkennen und behandeln [113].

Attack Impact Assessment

Ein Simulations-TB für cyber-physische Sicherheit in Verteilnetzen kombiniert Stromnetzmodelle in RTDS mit Network Simulator 3 (ns-3)-basierter Kommunikation und über Modbus angebundener SCADA-Steuerung. Dies ermöglicht Cyberangriffe auf die Steuerungsebene, deren Auswirkungen auf Spannungen, Ströme und andere Stromnetzvariablen untersucht werden, um die Auswirkungen unterschiedlicher Angriffsszenarien zu bewerten [171]. In einer Digital-Power-Twin-Umgebung für Smart Grids werden Angriffe gegen Netzkomponenten durchgeführt, die sowohl im physischen TB als auch im Echtzeit-Digital-Twin abgebildet sind. Deren Auswirkungen werden durch die Analyse von Anomalie-Alarmen anhand von International Electrotechnical Commission (IEC) 61850-Generic Object Oriented Substation Event (GOOSE)-Nachrichten sowie der entsprechenden Veränderungen im Netzbetrieb innerhalb des Twins bewertet [74].

Dataset Generation

Der SDN-DAD-Datensatz wird in einer Software-Defined Networking (SDN)-basierten Testumgebung generiert, indem legitimer Hypertext Transfer Protocol (HTTP)-Traffic, Flash-Events und mehrere Distributed Denial-of-Service (DDoS)-Angriffstypen mittels curl-loader und weiterer Tools orchestriert werden. Dabei werden Controller- und Flow-Level-Informationen erfasst, sodass der resultierende Datensatz die Forschung zu effizienten DDoS-Erkennungsmerkmalen unterstützen kann [77]. Ein logdaten-orientiertes TB für Cybersicherheitsexperimente nutzt skriptgesteuerte Nutzerinteraktionen mittels Selenium sowie kontrollierte Systemaktivitäten, um realistische, reproduzierbare Log-Traces zu erzeugen. Diese werden anschließend als öffentlich verfügbare Datensätze veröffentlicht, die zum Training und zur Evaluierung von Intrusion-Detection- und Analyseansätzen dienen [189].

Cyber Security Resilience Assessment

Ein resilienzfokussiertes TB modelliert einen mit einem autonomen Cyberabwehrsystem und physischen Resilienzmechanismen ausgestatteten Lkw und nutzt OpenTAP zur Automatisierung von Malware-Angriffsexperimenten. Dadurch lassen sich quantitative Cyber-Resilienz-Metriken ableiten, die zeigen, wie die kombinierten cyber- und physischen Schutzmaßnahmen die Funktionsfähigkeit unter anhaltenden Kompromittierungsversuchen aufrechterhalten [203]. Eine weitere Studie zu Schutz-Intelligent Electronic Devices (IEDs) verwendet einen Laboraufbau mit IEC 61850-GOOSE-Kommunikation, um Angriffe auf Protokollebene durchzuführen und die Reaktionen der Geräte zu beobachten. Dadurch wird die Resilienz unterschiedlicher kommerzieller IED-Implementierungen hinsichtlich ihrer Fähigkeit bewertet, GOOSE-basierten Störungen standzuhalten, diese zu erkennen und eine Wiederherstellung nach solchen Vorfällen zu gewährleisten [25].

Mitigation Strategies

Im hierarchischen SDN-DDoS-Abwehr-TB wird der generierte SDN-DAD-Traffic nicht nur zur Erkennung, sondern auch zur Bewertung von Mitigation-Strategien genutzt, die controllerübergreifend koordiniert werden. Dabei passt das System dynamisch Flow-Regeln basierend auf den Erkennungsergebnissen an, um Angriffs-Traffic zu begrenzen und gleichzeitig legitime Flash-Crowd-Anfragen zu erhalten [77]. Ein Echtzeit-Co-Simulations-TB für öffentliches Electric Vehicle (EV)-Laden verknüpft ein OPAL-RT-HYPERSIM-basiertes Stromnetzmodell mit EV-Infrastruktur und einer Monitoring-Plattform. Dies ermöglicht es den Autor*innen, EV-basierte Cyberangriffe einzuspielen und anschließend Mitigation-Strategien zu bewerten, die auf abnormale Netz- und Kommunikationsbedingungen reagieren, um einen stabilen Betrieb aufrechtzuerhalten [77].

ML-based IDS/IPS

Ein SDN-TB zur Abwehr von IoT-gesteuerten DDoS-Angriffen bettet ein semi-überwachtes Deep-Learning-Modell in den SDN-Controller ein. Dabei wird der durch curl-loader und Angriffstools generierte Traffic überwacht und von der ML-basierten Intrusion-Detection-Komponente klassifiziert, um legitime von bösartigen Flows zu unterscheiden und automatisierte Abwehrentscheidungen zu unterstützen [142]. Eine Security-Umgebung für Stromnetze, die oszillierende Lastangriffe von kompromittierten EV-Ladestationen modelliert, nutzt eine MATLAB/Simulink-Implementierung des IEEE-New-England-39-Bus-Systems zur Generierung cyber-physischer Datensätze. Diese werden anschließend von Deep-Learning-Modellen am Edge verarbeitet, um die Angriffe im Rahmen eines ML-basierten IDS für das Stromnetz zu erkennen und zu lokalisieren [156].

Anomaly Detection

Ein Smart-Grid-TB, aufgebaut um PLCs, rapid-SCADA, pySCADA und einen SQL-basierten Log-Server, unterstützt ein erklärbares, selbstbewusstes Framework zur Intrusion-Detection und aktiven Reaktion. Dabei erfolgt die Anomalieerkennung durch die Analyse der gesammelten Prozess- und Kommunikations-Traces des Stromnetzes, um verdächtiges Verhalten zu identifizieren und automatisierte Reaktionen auszulösen [215]. In einer CR-Plattform, die Nutzer- und Systemaktivitäten über verschiedene Services hinweg protokolliert, werden Process-Mining-Tools auf Event-Logs angewendet, um normale Prozessmodelle zu ermitteln und Abweichungen zu erkennen. Die Anomalieerkennung wird dabei als Conformance-Checking zwischen beobachteten CR-Ausführungs-Traces und erwartetem Prozessverhalten umgesetzt [24].

AI-based Anomaly Detection

Ein offenes Fifth-Generation Mobile Network (5G)/Open Radio Access Network (O-RAN)-TB basiert auf Komponenten wie Open5GS für das Kernnetz, einem RAN Intelligent Controller (RIC) sowie GNU Radio/GNU Radio Companion, einschließlich eines Flow-Graphen, der unterschiedliche Zustandsstufen für mehrere User Equipment (UEs) simuliert. Innerhalb dieser Umgebung stellen die Autor*innen einen neuartigen AI-basierten Ansatz zur Anomalieerkennung vor, der anhand des generierten Traffics evaluiert wird und darauf ausgelegt ist, eine nahezu verschwindende Falsch-Positiv-Rate bei sauberem Traffic zu erreichen [130]. Ein Co-Simulations-TB für dezentrale Energieressourcen kombiniert Echtzeit-Stromnetzsimulation in RTDS mit Netzwerkemulation in ns-3 und SCADA-Kommunikation über Modbus und setzt modellbasiertes Reinforcement Learning ein, um koordinierte cyber-physische Angriffsereignisse zu erkennen. Das erlernte Modell fungiert dabei als AI-basierter Anomaliedetektor, der Abweichungen vom normalen Netzbetrieb signalisiert [154].

Cyber Security Risk Assessment

Eine kooperative Smart-Farming-Umgebung kombiniert physische Systeme mit Digital Twins am Edge, wobei ein Digital Twin mittels Azure Digital Twins implementiert und anschließend Angriffen ausgesetzt wird, sodass sich Cyber- und Digital-Twin Verhalten beobachten lassen. Die resultierenden Smart-Farming-Netzwerkdatensätze werden zur Dataset-Generierung und AI-basierten Anomalieerkennung genutzt, um potenzielle Bedrohungen in diesem Umfeld zu identifizieren [133]. Ein Simulations-TB für cyber-physische Sicherheit dezentraler Energieressourcen nutzt Modbus-Kommunikation zwischen SCADA-Systemen in Leitstellen und Remote Terminal Units zusammen mit Echtzeitsimulation von Strom- und Kommunikationssystemen in RTDS sowie Netzwerkemulation in ns-3. Dadurch kann eine Cyber-Security-Risikobewertung durchgeführt werden, indem Cyberangriffe auf das simulierte Verteilnetz ausgeführt und deren Auswirkungen auf das Stromnetz analysiert werden [171].

Traffic Generation

Ein SDN-basiertes TB zur Abwehr von DDoS-Angriffen durch kompromittierte IoT-Geräte nutzt curl-loader zusammen mit weiteren Traffic-Tools, um große Mengen an HTTP-Anfragen und vielfältige DDoS-Muster zu generieren. Dadurch kann die semi-überwachte Erkennungs- und Mitigation-Logik des Controllers unter gemischten legitimen und Angriffs-Traffic-Bedingungen evaluiert werden [142]. Ein hierarchisches DDoS-Abwehrsystem für SDN-Netzwerke setzt ebenfalls auf curl-loader, um Flash-Crowd-HTTP-Traffic in großem Maßstab zu emulieren, und kombiniert diese generierte Last mit verschiedenen DDoS-Angriffen, um den SDN-DAD-Datensatz zu erstellen und zu bewerten, wie sich die vorgeschlagene mehrschichtige Abwehr unter unterschiedlichen Traffic- und Angriffskonfigurationen verhält [77].

4.2.2. Training and Exercises

Abbildung 6 fasst die zehn am häufigsten genannten *Use Cases* für den *Zweck* „Training and Exercises“ über CRs und TBs hinweg zusammen. Da ein einzelner Artikel mehrere *Use Cases* beschreiben kann, zählen die Balken Use-Case-Nennungen und nicht eindeutige Publikationen. Der Datensatz umfasst insgesamt 75 Nennungen. Die zehn am häufigsten genannten *Use Cases* machen 47 Nennungen aus (62,7 %). Alle übrigen *Use Cases* werden jeweils weniger als fünfmal genannt und sind daher nicht in der Abbildung dargestellt. Zusammen machen sie 28 Nennungen aus (37,3 %). Im Vergleich zu „Research, Testing and Experimentation“, wo TB dominiert (TB 84,3 %, CR 15,7 %), ist der *Zweck* „Training and Exercises“ deutlich CR-zentriert. CR macht 56 Nennungen aus (74,7 %), TB trägt 19 Nennungen bei (25,3 %). Innerhalb der Top 10 führt „Cyber Security Training: Capture the Flag“ mit 9 Nennungen, gefolgt von „Cyber Security Training: General“ mit 8 Nennungen. Die nächste Gruppe umfasst „Incident Response“ (6), „Cyber Security Training: Red Team vs. Blue Team“ (6) und „Gamification“ (6). Seltener genannte *Use Cases* sind „Cybersecurity Exercise Evaluation“ (5), „Cyber Security Training: Red Teaming“ (3) und „Cyber Security Training: Malware Attack and Defense“ (2), wobei „Crisis Management Training“ und „Cellular Botnets“ die Top 10 mit jeweils 1 Nennung abschließen. Insgesamt zeigt die Verteilung, dass trainingsorientierte Arbeiten überwiegend auf CRs durchgeführt werden, wobei TBs einen kleineren, aber sichtbaren Anteil beitragen.

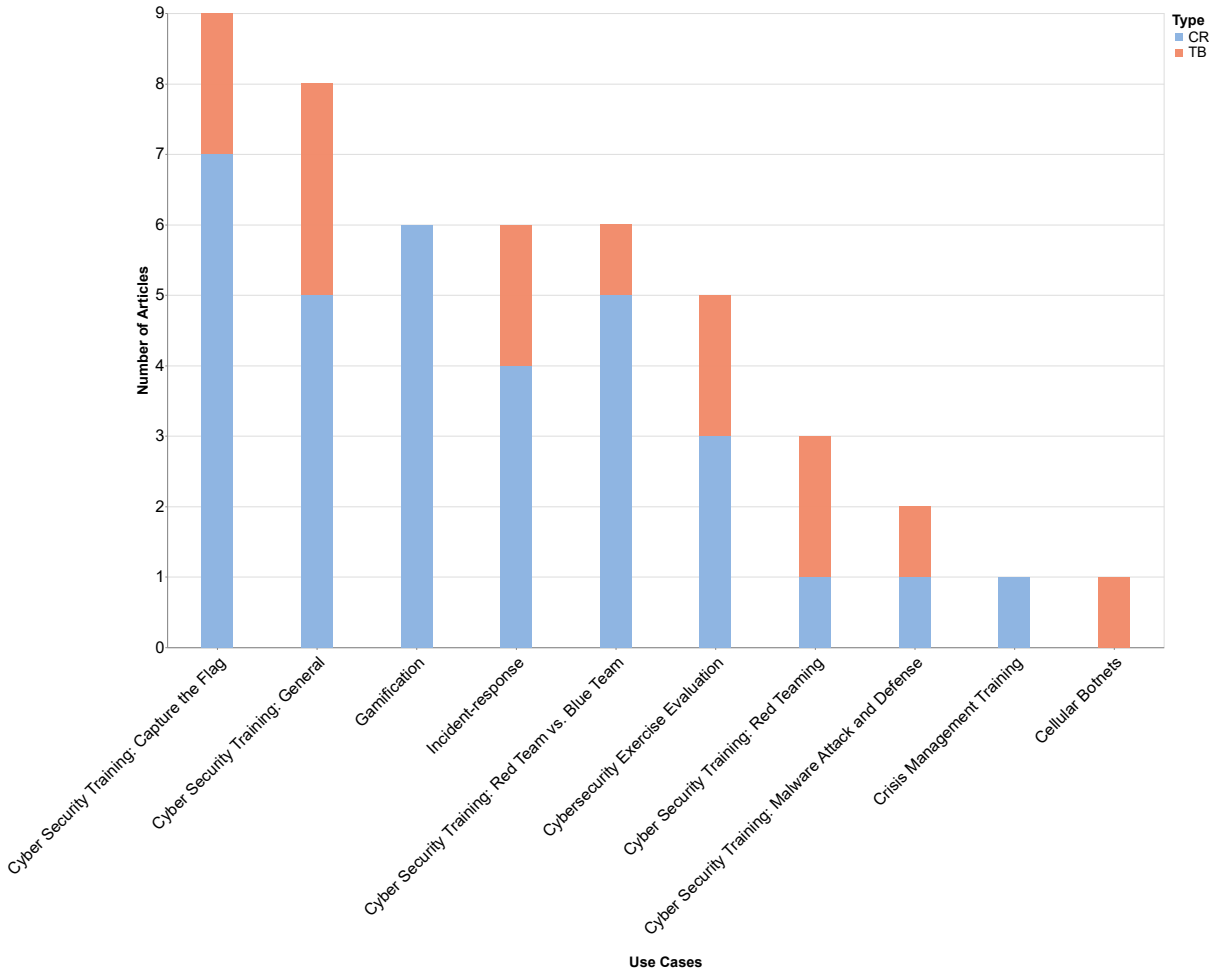


Abbildung 6: Top-10 Use Cases für den Zweck „Training and Exercise“ über Cyber Ranges (CR) und Testbeds (TB) hinweg.

Cyber Security Training: Capture the Flag
Ein Capture-the-Flag-*Use Case* wird auf dem TROY-TB umgesetzt, einer virtuellen IT- und OT-Umgebung, die auf einem VMWare-ESXi-Hypervisor mit dedizierten virtuellen Netzwerken und Maschinen entsprechend einer IT/OT-Referenzarchitektur gehostet wird. Dabei betreibt ein Typhoon-HIL-602+-Echtzeitsimulator hochpräzise Stromnetzmodelle kritischer Infrastrukturen (IEEE 4-, 13- und 33-Bus mittels ModbusTCP oder DNP3), Übungen im Klassenzimmer nutzen einen Teil des GRFICSv2-Frameworks mit einer grafischen Tennessee-Eastman-Prozesssimulation, SCADA und einer virtuellen PLC über OpenPLC, und Ignition SCADA bietet zusammen mit OPC-UA-Tags die SCADA/User Interface (UI)-Schicht, während NETLAB+ das Erstellen von Snapshots und das Zurücksetzen des virtuellen Labs ermöglicht, sodass Capture-the-Flag-Aufgaben wiederholt in einer realistischen Lernumgebung durchgeführt werden können [174]. Ein zweiter Capture-the-Flag-*Use Case* wird in der KYPO4INDUSTRY-Umgebung realisiert, die Linux-basierte virtuelle Maschinen, physische Industriegeräte mit Sensoren und Aktoren sowie mehrere Industrieprotokolle wie Message Queuing Telemetry Transport (MQTT) und REST kombiniert, sodass Studierende praxisnahe ICS-CTF-Übungen auf realistischer industrieller Steuerungsinfrastruktur durchführen können [31].

Cyber Security Training: General
Ein allgemeiner Trainings-*Use Case* basiert auf der Austrian Institute of Technology (AIT)-CR, die als modulare, OpenStack-basierte Umgebung konzipiert ist, in der CRs über Terraform, Consul und Git instanziiert und verwaltet werden. Dies ermöglicht die flexible Bereitstellung unterschiedlicher Trainingstopologien und Übungen für Ausbildung und Praxis im Bereich Cybersicherheit [91]. Ein weiterer allgemeiner Trainings-*Use Case* wird durch die akademische CR Tectonic bereitgestellt, die auf Cloud-Infrastruktur und Infrastructure as Code zur Bereitstellung realistischer Systeme und Netzwerke setzt, Elastic Security zur Überwachung und Alarmierung integriert und konfigurierbare Trainingsübungen unterstützt, die theoretische Lehre mit praktischen CR-Aktivitäten kombinieren [64].

Incident Response
Ein Incident-Response-*Use Case* wird in einem IoT-TB für Abwasserbehandlung realisiert, in dem IoT-Geräte ihren Zustand über MQTT veröffentlichen und die erfassten Daten entsprechend der Netzwerkaktivitäten gespeichert und gelabelt werden. Dies ermöglicht es, Incident-Handling- und Erkennungs-Workflows anhand realistischer Prozess- und Kommunikations-Traces aus der Aufbereitungsumgebung zu üben [32]. Ein Incident-Response-*Use Case* wird in einer CPS-TB-basierten QRGridEx-Umgebung realisiert, in der ein Echtzeit-Digitalsimulator für Stromnetze mit standardmäßiger SCADA-Kommunikation und integrierten Intrusion- und Anomalieerkennungssystemen kombiniert wird, sodass Cyberangriffe auf das Netz durchgeführt und deren Erkennung und Handhabung über die gekoppelte cyber-physische Infrastruktur hinweg analysiert werden können [145].

Cyber Security Training: Red Team vs. Blue Team
Ein Red-Team-vs.-Blue-Team-*Use Case* basiert auf dem CRACK-Framework, das auf einem über Apache ARIA orchestrierten, OpenStack-basierten TB läuft und Netzwerksicherheitsübungen bereitstellt, bei denen ein Red Team mehrstufige Dienste angreift (zum Beispiel ein Apache-basiertes Web-Server-Frontend und interne Server) und das Blue Team diese Aktivitäten innerhalb der emulierten Infrastruktur verteidigt und analysiert [151]. Red-Team-vs.-Blue-Team-Training wird durch die DefAtt-Plattform unterstützt, eine stark automatisierte CR, die virtuelle Maschinen und Container als vernetzte Ziele bereitstellt und zentrale Logging- und Analysekomponenten nutzt, um strukturierte Übungen mit Fokus auf netzwerkbasierte Angriffe und deren Abwehr

durchzuführen, während gleichzeitig Skalierbarkeitstests der Übungsumgebung ermöglicht werden [104].

Gamification

In einem Gamification-*Use Case* nutzt eine industrielle Cybersicherheitsumgebung Remote-Access-Labore mit industrieller Steuerungsausrüstung und Kommunikationsinfrastruktur zur Vermittlung von Cybersicherheitsausbildung, wobei Gamification erreicht wird, indem industrielle Kommunikations- und Prozesssteuerungsaufgaben in strukturierte Challenges innerhalb des Trainingsaufbaus umgewandelt werden [87]. Ein weiterer gamifizierter *Use Case* findet sich in der NITRO-5G-IoT-CR, die ein echtes 5G-Kernnetz und verbundene IoT-Systeme emuliert und generierten Netzwerkverkehr sowie 5G-Dienste nutzt, um spielähnliche Übungen zu erstellen. Dies ermöglicht es Teilnehmenden, Sicherheitsaspekte durch gamifizierte Interaktionen mit der emulierten 5G–IoT-Umgebung zu testen, zu analysieren und zu verfeinern [58].

Cybersecurity Exercise Evaluation

Ein *Use Case* zur Übungsevaluierung nutzt ein Cyber-Range-Framework, das viele Aufgaben bei der Durchführung von Cybersicherheitsübungen automatisiert. Dabei werden Szenarien über eine JavaScript Object Notation (JSON)-basierte domänenspezifische Sprache und Datalog-Spezifikationen modelliert und ausgeführt, und CTFd wird für Scoring und Instrumentierung eingesetzt, sodass die Leistung der Teilnehmenden und Übungseigenschaften systematisch analysiert werden können [207]. Ein weiterer *Use Case* zur Übungsevaluierung wird in einer Implementierungs- und Evaluierungsmethodik für Cyber Ranges beschrieben, die Process-Mining-Tools nutzt, um Event-Logs aus Trainingsübungen zu analysieren. Dabei kommen Plattformen wie Moodle und weitere Monitoring-Komponenten zur Datenerfassung zum Einsatz, um Cyber-Range-Trainings und Ausbildungsprozesse aus unterschiedlichen Perspektiven zu evaluieren [63].

Cyber Security Training: Red Teaming

Ein Red-Team-Trainings-*Use Case* wird durch ein SCADA-Cybersicherheitsschulungs- und Sensibilisierungsprogramm bereitgestellt, das auf zwei Zwillings-CRs, WonderICS und G-ICS, aufbaut. Dabei ermöglichen ein Advanced Persistent Threat (APT)-Demonstrator und eine flexible Laborumgebung es den Teilnehmenden, das Angreifen und Verteidigen industrieller Steuerungssysteme in praxisnahen Übungen und studentischen Pentesting-Sessions zu üben [137]. Dockerized Android richtet eine containerbasierte CR-Umgebung für mobile Geräte ein, in der Android-Emulator-basierte Geräte und zugehörige Dienste über Docker bereitgestellt werden, um realistische, verwundbare mobile Szenarien für Red-Team-Übungen zu erstellen. Eine Web-UI mit React.js-Frontend und Nginx/Node.js-Backend bietet koordinierten Zugriff auf diese emulierten Geräte und verwundbare Anwendungen wie die App Wi-Fi Baby Monitor, sodass Threat- und Vulnerability-Assessment als strukturierte Red-Teaming-Trainings-*Use Cases* durchgeführt werden können [30].

Cyber Security Training: Malware Attack and Defense

Ein maritimer *Use Case* für Malware-Angriff und -Abwehr wird auf dem virtuellen TB MaCySTe realisiert, das die Bordnetzwerkinfrastruktur und zentrale Komponenten schiffsbasierter cyber-physischer Systeme nachbildet, indem es sich mit einem angepassten Bridge-Command-Schiffssimulator verbindet, der Simulationsdaten über einen Message-Queuing-Aufbau austauscht, während eine Datenerfassungseinheit und eine Radarantenne Sensordaten als Multicast-UDP mittels National Marine Electronics Association (NMEA)- und BR24/Asterix-Protokollen übertragen. Die Umgebung kombiniert PLC-Simulation mit OpenPLC über Modbus, FUXA-basierte

Human–Machine Interfaces (HMIs), Radar-Overlay-Funktionalität über NATS und OpenCPN sowie containerisierte, mit Podman, Flatpak, GNU-Make-Task-Automatisierung und OpenSearch-basierter Indizierung bereitgestellte Dienste. Dies ermöglicht realistisches Cybersicherheitstraining für maritimes Personal mit Fokus auf maritime Cyberbedrohungen und Auswirkungsbewertung innerhalb eines dedizierten TB [99]. Eine CR-Smart-Assistant-Umgebung wird für Training zu Malware-Angriff und -Abwehr genutzt, bei der Studierende über eine auf Yandex.Dialogs basierende Schnittstelle mit der CR interagieren, die als Frontend zur Anforderung von Lehrmaterial und zum Erhalt von Anleitung durch einen virtuellen Assistenten dient, der auf einer Cybersicherheits-Ontologie basiert. Dadurch können Trainingsaktivitäten über Learning-Management-, Instructional-Design- und Scoring-*Use Cases* für Studierende hinweg unterstützt und bewertet werden [214].

Crisis Management Training

Crisis-Management-Training wird in einer auf OpenStack basierenden CR umgesetzt, in der mehrere Windows-10-Client-Rechner, Server (einschließlich File Transfer Protocol (FTP)- und Virtual Network Computing (VNC)-basiertem Verwaltungszugriff) und überwachte Endpunkte realistischen Netzwerkverkehr erzeugen. Ein dedizierter Traffic-Generierungsaufbau wird eingesetzt, sodass Organisationen und Entscheidungsträger*innen im Umgang mit Krisenreaktion und Entscheidungsfindung unter simulierten Cybervorfällen geschult werden können [150].

Cellular Botnets

Ein *Use Case* zu Cellular Botnets wird auf dem virtuellen End-to-End-5G-Netzwerk-TB VET5G umgesetzt, in dem containerisierte 5G-Kernnetzfunktionen, gNodeBs (gNBs) und UEs mit Kubernetes und Docker orchestriert werden. UEs werden dabei mittels Android-Emulator-Instanzen mit Android 11 und 5G-Unterstützung emuliert, und Komponenten wie der gNB-Emulator von OAI, ein P4-BMv2-Software-Switch, Open Authorization (OAuth)-2.0-basierter Dienstzugriff, MongoDB, Wireshark, tcpdump, Bettercap, Metasploit, Hydra, sFuzz, wfuzz und JupyterHub werden kombiniert, um Cybersicherheitsübungen mit der Bezeichnung „Slicing Attacks, Cellular Botnets“ für Attack-Impact-Assessment sowie Testbed-Design und -Evaluierung innerhalb von 5G- und Sixth-Generation Mobile Network (6G)-Sicherheits-*Use Cases* zu unterstützen [205].

4.2.3. Education

Abbildung 7 fasst die im Bereich Education beobachteten *Use Cases* über CRs (CR) und TBs (TB) hinweg zusammen. Da ein einzelner Artikel mehrere *Use Cases* beschreiben kann, zählen die Balken Use-Case-Nennungen und nicht eindeutige Publikationen. Der Datensatz umfasst insgesamt 43 Nennungen über fünf *Use Cases*. Über die Plattformtypen hinweg dominieren CRs mit 34 Nennungen (79,1 %), gefolgt von TBs mit 9 (20,9 %), was darauf hindeutet, dass bildungsorientierte Aktivitäten am häufigsten auf CRs durchgeführt werden. Unter den einzeln benannten *Use Cases* führt „Student Assessment & Scoring“ mit 15 Nennungen und wird ausschließlich auf CRs beobachtet. „Learning Management System“ folgt mit 13 Nennungen, und „Instructional Design“ verzeichnet 12 Nennungen, wobei beide primär auf CRs, aber auch auf TBs vertreten sind. Seltenere Aktivität umfasst „Learning Labs“ mit 2 Nennungen (beobachtet auf TBs) und „Resource Development“ mit 1 Nennung. Insgesamt werden Education-*Use Cases* primär auf CRs umgesetzt, während TBs vor allem zu Learning-Management- und Instructional-Design-Arbeiten beitragen und die begrenzte Learning-Labs-Aktivität abdecken.

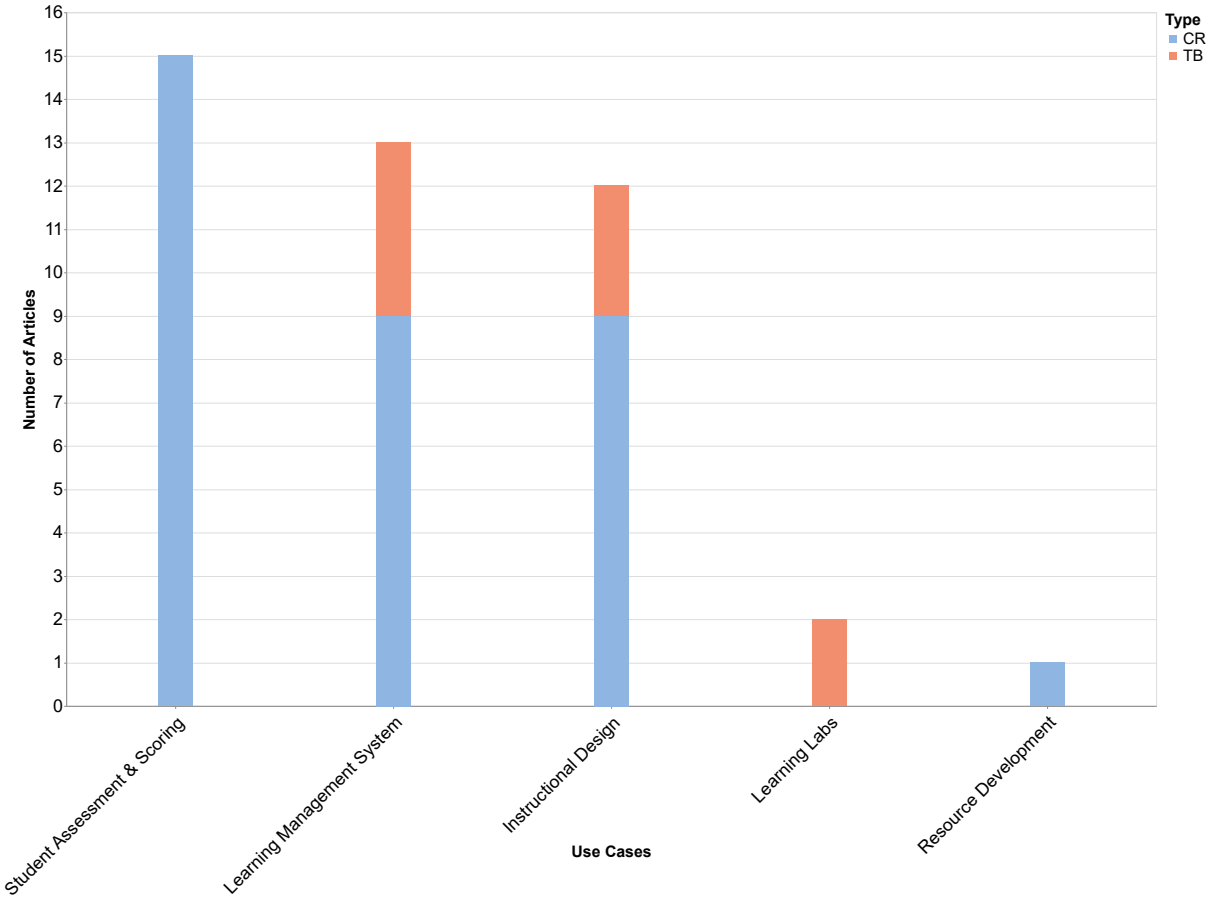


Abbildung 7: Top-Use-Cases für den Zweck „Education“ über Cyber Ranges (CR) und Testbeds (TB) hinweg.

Student Assessment & Scoring

Ein CR-Smart-Assistant-Dienst wird basierend auf der Analyse digitaler Fußabdrücke von Studierenden entwickelt und stellt Lehrmaterial und Ratschläge über eine interaktive Anfrage-Antwort-Schnittstelle bereit [214]. Die CR BUTCA implementiert einen ereignisbasierten *Use Case* zur Datenerfassung und -analyse auf einer OpenStack-betriebenen Plattform, einschließlich eines Authentifizierungsservers und proprietärer Webanwendungen für Plattformverwaltung und Cybersicherheits-Use-Cases. Monitoring und Dashboards werden mit Prometheus und Grafana unterstützt. Die Orchestrierung erfolgt über Ansible AWX, und für zentrales Log-Management kommt Kibana mit Elasticsearch zum Einsatz. Nach der Analyse werden die ausgewerteten Daten der Web-Benutzeroberfläche beispielsweise in JSON zur Instanz- und Use-Case-Übersicht mit clientseitigem Rendering bereitgestellt [89].

Learning Management System

Ein CR-System automatisiert viele Aufgaben von Cybersicherheitsübungen und unterstützt die Autonomie und Kompetenzentwicklung der Teilnehmenden. Es basiert auf einem Open-Source-Bereitstellungsansatz auf Basis von OpenStack, der auf Cloud-Infrastrukturen laufen kann, ohne auf Drittanbieter-Infrastruktur angewiesen zu sein [207]. IoT-Sicherheitstraining wird über eine Methodik organisiert, die ein tiefgehendes Verständnis von IoT durch praxisnahes Üben anstrebt. FIT IoT-LAB wird in diesem Learning-Management-Kontext als TB-Infrastruktur für IoTrain-Lab eingesetzt [18].

Instructional Design

Eine Industrie-4.0-CR-Plattform wird entwickelt, um Übungen wie Snort-Regelerstellung, forensische Analyse und Man-in-the-Middle-Spoofing zu unterstützen. Die Umgebung nutzt eine isolierte Netzwerkinfrastruktur mit Virtual Private Network (VPN)-Zugang, um Alarme auszulösen und Log-Dateien für diese Aktivitäten zu generieren [193]. Ein interdisziplinärer Ansatz zur Gestaltung von CR-Übungen führt ein Cyber Range Exercise (CRX) für Incident Response ein. Das dabei eingesetzte Learning-Management-System ist mit VueJS implementiert und über eine mit Flask umgesetzte REST-Application Programming Interface (API) mit der Docker-Infrastruktur verbunden [60].

Learning Labs

TROY wird als vielseitiges Cybersicherheits-TB vorgeschlagen, um Daten- und Fachkräftemangel zu adressieren, und dient dem Vergleich quelloffener Cybersicherheits-Datensätze und TBs. Der Learning-Lab-Kontext wird zusammen mit Laborumgebungen diskutiert, die einen mit vSphere verwalteten Hypervisor sowie NETLAB+-Netzwerklabor-Tools nutzen [159]. Das TB TROY stellt eine virtuelle IT- und OT-Umgebung bereit, die mit einem Typhoon-HIL-Echtzeitsimulator zur Emulation kritischer Infrastrukturen ausgestattet ist. IEEE-4-Bus (ModbusTCP oder DNP3) und IEEE-13-Bus-Konfigurationen werden in dieser Laborumgebung als Standards für die Stromnetztopologie verwendet [174].

Resource Development

Eine OT-fokussierte CR wird unter Verwendung von VirtualBox-basierten virtuellen Maschinen entwickelt. Windows 10, Ubuntu und Kali Linux laufen in diesem Resource-Development-Aufbau als virtuelle Maschinen auf VirtualBox [155].

4.3. Technologien

Dieser Abschnitt beschreibt Technologien und ihre Anwendungsfälle in CRs und TBs, eingeteilt in *Technology Domains* und *Technology Subdomains*. Insgesamt werden 10 *Technology Domains* behandelt, die sich über die drei Layer von CRs oder TBs erstrecken: Core Technology, Orchestration und Target Infrastructure. Diese Domänen umfassen Red Team Operations, Data Storage, Monitoring and Analytics, Computing Platform, Custom Development, Blue Team Operations, Portal Services, Management, Network Infrastructure und Scenario.

Zu Beginn jedes Unterkapitels visualisiert eine Heatmap die Menge und Vielfalt der innerhalb der jeweiligen Domäne behandelten Technologien. Pro *Technology Domain* werden anschließend die *Technology Subdomains*, welche die zugehörigen Anwendungsfälle repräsentieren, anhand konkreter Implementierungsbeispiele beschrieben. Angesichts der umfangreichen Anzahl an Technologien und Publikationen stellt jede Subdomäne bis zu zwei der am häufigsten eingesetzten Technologien vor, jeweils beschrieben anhand von bis zu zwei Publikationen. Am Ende listet eine zusammenfassende Tabelle die Top-Technologien je Subdomäne auf. Die folgenden Unterkapitel behandeln jeweils eine dieser Domänen einzeln.

4.3.1. Red Team Operations

Insgesamt dominiert ICT den Einsatz von Red-Team-Operations-Technologien mit 116 Vorkommen, gefolgt von ICS (70) und IoT/IIoT (56). Power Systems (27), RAN & Mobile Devices (24) und CPS (19) treten seltener auf, während Intelligent Transportation Systems (3) nur spärlich vertreten ist. ICT weist in allen 13 Red-Team-Operations-Subdomänen von null verschiedene

Werte auf, und ICS, IoT/IIoT sowie RAN & Mobile Devices decken jeweils ein breites Spektrum an Subdomänen ab, was darauf hindeutet, dass diese *Anwendungsbereiche* übliche Ziele für Red-Team-Operations-Experimente sind. Über alle *Anwendungsbereiche* hinweg sind Training and Practice Systems (70), Network Scanning and Reconnaissance (61) und Exploitation and Attack Execution (59) die am häufigsten berichteten Subdomänen. Allein ICT zeigt 28 Nennungen bei Training and Practice Systems sowie jeweils 18 Nennungen bei Network Scanning and Reconnaissance und Exploitation and Attack Execution aus. ICS trägt zusätzliche Werte in denselben Subdomänen bei: 18 bei Training and Practice Systems, 14 bei Network Scanning and Reconnaissance und 15 bei Exploitation and Attack Execution. Darüber hinaus treten Attack Strategy & Support (31), Denial of Service & Distributed Denial of Service (29) und Paketmanipulation (18) regelmäßig auf, hauptsächlich in ICT, ICS und IoT/IIoT. Ein sekundärer Cluster wird durch Vulnerability Management (14), Password Cracking and Credential Harvesting (11) und Brute Force Attacks (9) gebildet. Spezialisiertere Aktivitäten bleiben selten. Adversary Emulation (5) und Reverse Engineering and Binary Analysis (4) treten nur vereinzelt auf, während Phishing and Social Engineering (2) sowie Proxy and Web Interception (2) nahezu nicht vorhanden sind. Insgesamt zeigt die Heatmap 8, dass die untersuchten CRs und TBs primär Trainingsaktivitäten sowie auf Reconnaissance und Exploitation fokussierte Red Team Operations unterstützen, während Adversary-Emulation- und Social-Engineering-Aktivitäten in der Literatur deutlich seltener vertreten sind.

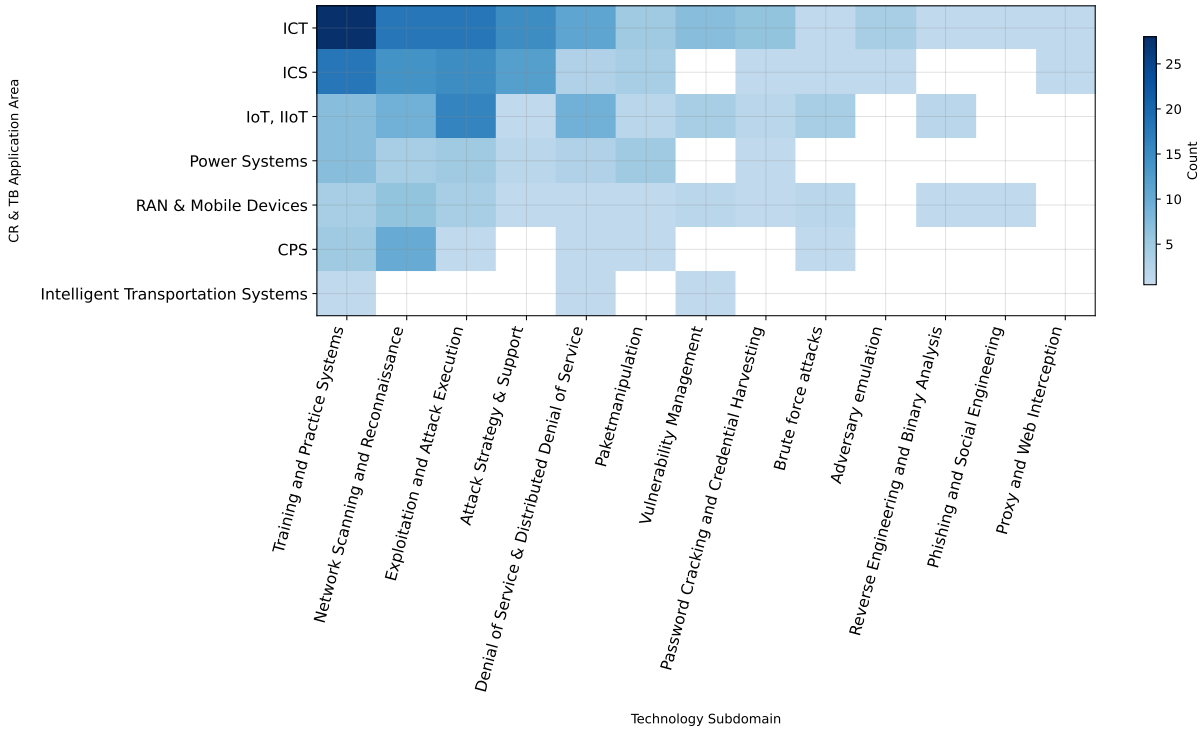


Abbildung 8: Verteilung der Red-Team-Operations-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Training and Practice Systems

MySQL wird eingesetzt, um Anwendungen für SQL-Injection-Übungen zu hosten, sodass Trainierende in einer ICS-orientierten CR das Erkennen und Ausnutzen von Injection-Schwachstellen üben können [193]. Das CR-Framework CRACK umfasst einen Apache-Webserver in einem Netzwerksicherheitsszenario, in dem ein falsch konfigurierter Reverse-Proxy ausgenutzt wird. Dadurch können Trainierende Reconnaissance- und Exploitation-Workflows gegen ein Web-Frontend üben, das Zugriff auf interne Dienste innerhalb der emulierten Infrastruktur bietet [151]. In einer

Raspberry-Pi-basierten CR wird Damn Vulnerable Web Application (DVWA) als beispielhafte verwundbare Webanwendung bereitgestellt, um zu bewerten, wie effektiv die Range Threat-and-Vulnerability-Assessment-Übungen für Webanwendungen unterstützt. So können Lernende in einem kompakten Trainingsaufbau Angriffe und Verteidigungsmaßnahmen durchführen [139]. Eine verteilte IoT/IIoT-TB-Architektur integriert DVWA als verwundbares Web-Frontend für bestimmte Szenarien der TON_IoT-Datensätze, wobei offensive Systeme die Anwendung mit unterschiedlichen Techniken angreifen, sodass gelabelte Telemetrie- und Netzwerkverkehrsdaten für die AI-basierte Sicherheitsevaluierung erfasst werden können [112].

Network Scanning & Reconnaissance

Eine Studie zur Abwehr von Drohnenüberwachung nutzt Nmap und Wireshark für Network Scanning and Reconnaissance: Nmap führt detaillierte Scans der identifizierten Zieldrohne durch, während Wireshark den zugehörigen Netzwerkverkehr innerhalb der Drohnenüberwachungs-TB-Umgebung erfasst und analysiert, um die Bewertung der Angriffseffektivität und der Abwehrmaßnahmen zu unterstützen [198]. Ein emuliertes TB für industrielle Steuerungssysteme zur Analyse fortgeschrittener Cyberbedrohungen setzt Nmap ein, um Schwachstellen in ICS-Komponenten zu identifizieren, sowie Wireshark, um den Demilitarised Zone (DMZ)-Netzwerkverkehr zu überwachen und zu analysieren. Dies ermöglicht die Identifikation verdächtiger Kommunikationsmuster in realistischen ICS-Szenarien [52].

Exploitation and Attack Execution

Eine Studie zur Anomalieerkennung für luftisolierte industrielle Steuerungssysteme in Kernkraftwerken nutzt Metasploit, um vorgefertigte Modbus/TCP-Angriffsmodule gegen die Benutzeroberfläche und den Controller auszuführen, während Ettercap Man-in-the-Middle-Angriffe im selben ICS-TB durchführt, um bösartigen Traffic für das Training und die Validierung des Erkennungsmodells zu erzeugen [181]. Eine SCADA-Sicherheitsstudie zu verdeckten Eindringversuchen in Modbus-basierte Systeme setzt Ettercap ein, um Address Resolution Protocol (ARP)-Poisoning-Angriffe durchzuführen. Dies ermöglicht unauffällige Hijacking- und Blackout-Szenarien in einer SCADA-Umgebung und erzeugt Traces, die veranschaulichen, wie Schwachstellen auf Protokollebene ausgenutzt werden können, während sie schwer zu erkennen bleiben [197]. Eine auf VMware-VMs basierende ICS-CR nutzt Metasploit als zentrales Penetrationstest-Framework: Nach der Bereitstellung mehrerer Zielrechner führt ein Kali-Linux-Angreiferhost Metasploit aus, um verwundbare Dienste im industriellen Netzwerk auszunutzen. Dies unterstützt praxisnahes Training und Vulnerability Assessment in der emulierten ICS-Umgebung [100].

Attack Strategy and Support

Eine virtuelle ICS-Umgebung für Abwasserbehandlung nutzt MITRE ATT&CK als Threat-Emulation-Tool, um Angreiferverhalten gegen bestimmte industrielle Automatisierungsebenen zu strukturieren und auszuführen. Dies ermöglicht die systematische Analyse der Auswirkungen von Modbus/TCP-Protokollangriffen auf den Prozess [101]. Die akademische CR Tectonic übernimmt MITRE ATT&CK als Grundlage zum Aufbau von Bedrohungsmodellen und Regelwerken, sodass Angriffsregeln mit Techniken, Taktiken und Vorgehensweisen aus dem Framework erweitert und zur Erkennung von Verhaltensweisen der Studierenden in automatisierten Trainingsszenarien genutzt werden können [64]. In einem emulierten TB für industrielle Steuerungssysteme wird iptables zur Traffic-Umleitung konfiguriert, wobei Kommunikation, die normalerweise zwischen HMI und PLC fließt, umgeleitet wird, sodass sie stattdessen über einen Angreiferhost läuft, um Cyberbedrohungsexperimente in realistischen ICS-Szenarien durchzuführen [52]. Ein Framework zur Generierung von 5G/6G-Sicherheitsdatensätzen nutzt iptables in einem Man-in-the-Middle-Szenario, indem Forwarding-Regeln auf der Angreiferentität hinzugefügt werden. Dies ermöglicht

das Abfangen und Manipulieren von Traffic beim Erstellen persistenter Protocol Data Unit (PDU)-Session-Angriffs-Traces auf IP-Schicht und im Kernnetz [10].

Denial of Service & Distributed Denial of Service

Ein IoT-Forensik-TB zur Cyberangriffsattribution nutzt Hping und scapy als Traffic-Generierungstools, um TCP-SYN-Flood- und SMURF-Angriffsverkehr in einem IoT/IIoT-Netzwerk zu erzeugen. Dabei entstehen bösartige Traces, die in den IoT-CAD-Datensatz für Attributionsexperimente aufgenommen werden [110]. In einer Sicherheitsstudie zu kooperativem Smart Farming wird Hping als Denial-of-Service-Tool eingesetzt, um TCP-SYN-Flood-Angriffe gegen Smart-Farming- und Digital-Twin-Komponenten zu starten. Dies unterstützt die Erstellung von Datensätzen, die Bedrohungen für landwirtschaftliche Edge- und Digital-Twin-Architekturen erfassen [133]. Ein HiL-TB zur Simulation von Anlagen für erneuerbare Energien nutzt scapy als Netzwerkinteraktionsbibliothek, um S7-Protokollpakete zu erstellen, zu zerlegen und zu manipulieren. Dies ermöglicht eine detaillierte Steuerung und Modifikation von industriellem Steuerungsverkehr bei der Analyse von Datenmanipulationsangriffen in Cybersicherheitsexperimenten für Stromsysteme [79].

Packet Manipulation

Eine Studie zu föderiertem Transfer Learning für Netzwerkanomalieerkennung nutzt Ettercap als Packet-Manipulation-Tool, um ARP-Poisoning-Angriffe von einem Kali-Linux-Angreiferhost aus durchzuführen und manipulierten Traffic zur Evaluierung des vorgeschlagenen Abwehransatzes zu erzeugen [134]. In einer Digital-Power-Twin-Umgebung für Cybersicherheit von Stromsystemen wird Ettercap in die Komponenten Attack Designer und Launcher integriert, wobei dessen API genutzt wird, um Man-in-the-Middle-Angriffe durch gezielte Paketmanipulation gegen die emulierte Kommunikation des Stromsystems durchzuführen [74]. Ein HiL-TB für Angriffe auf das Siemens-S7-Protokoll setzt scapy als Packet-Manipulation-Framework ein, wobei Angriffsskripte S7-Kommunikationsframes für detaillierte Netzwerkinteraktion während ICS-Angriffsexperimenten definieren, zerlegen und erstellen [79]. Das modulare SCADA-Sicherheits-TB SCASS nutzt scapy, um False-Data Injection (FDI)-Angriffe durch das Erstellen und Injizieren modifizierter Protokollnachrichten umzusetzen. Dies ermöglicht die systematische Untersuchung von FDI-Angriffstechniken in industriellen Steuerungsumgebungen [44].

Vulnerability Management

Eine Cyber-Übungsplattform, die containerbasierte Virtualisierung mit anderen Bereitstellungsoptionen vergleicht, nutzt Owasp Zap (Zed Attack Proxy) und SkipFish als Schwachstellenscanner für Webanwendungen. Jeder Server wird als verwundbare Umgebung vorbereitet, und beide Tools werden eingesetzt, um die gehosteten Webanwendungen auf Schwachstellen zu scannen, sodass die Studie deren Verhalten über unterschiedliche physische und virtuelle Aufbauten hinweg vergleichen kann [118]. Eine quelloffene Plattform zur Analyse kommerzieller IoT-Geräte setzt Owasp Zap (Zed Attack Proxy) und SkipFish ein, um Informationen zu sammeln und die von den Geräten bereitgestellten Web-Schnittstellen auf Schwachstellen zu scannen. Die Tools werden vor den Hauptexperimenten ausgeführt, um nach Geräteschwachstellen und zugehörigen Exploit-Versuchen zu suchen, und unterstützen so die systematische Sicherheitsbewertung der verbundenen Geräte [2].

Password Cracking & Credential Harvesting

Ein CR-Szenario-Framework nutzt Hydra als Password-Cracking-Tool, damit ein Red Team Angriffe simulieren kann, die versuchen, das Passwort eines Managers mithilfe der rockyou-Wortliste wiederherzustellen. Dies integriert Credential-Angriffe in die skriptgesteuerte Szenarioausführung

innerhalb der CRACK-Umgebung [151]. Das digital-forensische TB IoT-CAD setzt Hydra als Passwortangriffs-Tool ein, das ein Admin-Konto auf einem ausgewählten Host mithilfe einer zuvor im Workflow generierten Wortliste angreift. Dies erzeugt Credential-Angriffsverkehr für AI-basierte Experimente zur Cyberangriffsattribution in IoT-Umgebungen [110]. Ein TB zur Generierung von Logdaten für Cybersicherheitsexperimente nutzt Mimikatz als Credential-Harvesting-Tool in Adversary-Emulation-Szenarien, in denen typische Angreiferschritte mit gängigen Sicherheitstools umgesetzt werden, sodass realistische Host- und Netzwerklogs für die Intrusion-Detection-Forschung erfasst werden können [189]. Eine Cyber-Übung im EPIC-Microgrid-TB integriert Mimikatz als Credential-Dumping-Tool, um credentialbezogene Operationen gegen SCADA- und Firewall-Komponenten durchzuführen. Dies ermöglicht es Trainierenden, Credential-Compromise-Szenarien in einem Stromsystemkontext zu beobachten und darauf zu reagieren [96].

Brute Force Attacks

Eine IoT/IIoT-TB-Architektur zur Evaluierung AI-basierter Sicherheitssysteme am Edge nutzt Hydra und Cewl als Brute-Force-Angriffstools. Cewl, als Tool zur Wortlistengenerierung für Brute-Force-Angriffe klassifiziert, wird mit Hydra, einem Password-Cracking-Tool, kombiniert, um automatisierte Passwort-Hacking-Szenarien gegen verwundbare Knoten im TB zu starten. Dies erzeugt realistische Credential-Angriffsdaten für die TON_IoT-Datensätze [112]. Im digital-forensischen TB IoT-CAD dient Cewl erneut als Wortlistengenerierungs-Tool, indem Website-Inhalte gecrawlt werden, um individuelle Passwortlisten zu erstellen, während Hydra als Passwortangriffs-Tool das Admin-Konto gegen diese generierte Wortliste testet. Gemeinsam setzen sie Brute-Force-Passwortangriffe um, die bösartigen Traffic zur Evaluierung von Methoden zur Cyberangriffsattribution in IoT-Umgebungen erzeugen [110].

Adversary Emulation

Ein TB für APT-Forschung nutzt MITRE Caldera als Adversary-Emulation-Tool, um APTKampagnen durchzuführen. Dabei wird dessen Skalierbarkeit und Anpassungsfähigkeit genutzt, um realistische Angriffsaktivität für den Aufbau eines umfassenden APT-Datensatzes zu erzeugen und die Entwicklung robuster Abwehrmaßnahmen zu unterstützen [175]. Die akademische CR Tectonic integriert MITRE Caldera als Tool zur Automatisierung von Angriffen in Trainingsszenarien, wobei es mit Monitoring-Diensten kombiniert wird, sodass Lehrende die Leistung der Studierenden bewerten können, während Caldera konfigurierbare Angriffskampagnen innerhalb der CR-Umgebung steuert [64]. Infection Monkey wird als Adversary-Emulation-Tool für Angriffs- und Breach-Simulation in einem Framework zur Automatisierung von Sicherheitsszenarien eingesetzt, wo es als eine der Anwendungen fungiert, die Red-Team-Fähigkeiten bereitstellen, um die Sicherheitsbereitschaft von Organisationen gegen reale Cyberangriffe zu testen und zu verbessern [3].

Phishing and Social Engineering

Eine Docker-basierte Android-Plattform für mobilgeräte-fokussierte CRs nutzt Gophish als Simulationstool für Phishing-Kampagnen. Gophish ist als Webanwendung integriert, die Phishing-E-Mails erstellt und versendet, wobei eine dockerisierte Version im Framework enthalten ist, um Phishing- und Social-Engineering-Übungen für mobile Geräte zu unterstützen [30]. Eine Fallstudie zur Abmilderung von Injection- und Phishing-Angriffen setzt ZPhisher als Phishing- und Social-Engineering-Tool ein, um Phishing-Websites zu erstellen. Diese Phishing-Seiten werden in Experimenten eingesetzt, die Sicherheitsangriffe im Zusammenhang mit Injection und Phishing analysieren und bewerten, wie Inspection-Plugins zur Umsetzung einer sichereren Umgebung beitragen können [23].

Reverse Engineering and Binary Analysis

Ein automatisiertes IoT-Sicherheits-TB integriert Binwalk als Reverse-Engineering-Tool für das Threat and Vulnerability Assessment von Firmware, wobei Gerätefirmware untersucht wird, um veraltete und damit potenziell verwundbare Versionen zu identifizieren. Im selben TB wird Dex2jar als Reverse-Engineering-Tool für mobile Anwendungen eingesetzt, um Android-Apps zu disassemblieren und zu prüfen, ob sie fest codierte Zugangsdaten enthalten, was als Schwachstellenindikator gewertet wird. Beide Tools sind Teil einer quelloffenen Plattform zur Analyse kommerzieller IoT-Geräte und zur Erkennung von Angriffen auf diese [2].

Proxy and Web Interception

Eine ICS-Sicherheitsstudie zu Abwasserbehandlung nutzt Ettercap als Proxy- und Web-Interception-Tool, um Integritätsangriffe durch das Abfangen und Manipulieren von Kommunikation im industriellen Steuerungsnetzwerk durchzuführen. Dabei werden eigenständige und hybride SDN-basierte Abwehrmaßnahmen gegen Kanalangriffe in einer Wastewater Treatment Plant (WWTP)-Fallstudie bewertet [102]. Ein TB für Multicast-Netzwerksicherheit setzt Owasp Zap (Zed Attack Proxy) als Proxy- und Web-Interception-Tool ein, um bösartigen Web-Traffic zu erzeugen und Angriffs-URLs über dessen Browser-Plug-in festzulegen. Dies ermöglicht die Leistungsbewertung von Firewalls und Sicherheitsmechanismen unter unterschiedlichen Angriffs- und Netzwerkkonfigurationen [188].

Tabelle 1: Top-10-Technologien je Subdomäne für Red Team Operations. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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 Modeling 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

4.3.2. Data Storage

Datenbanken und andere Datenspeichertechnologien werden über alle CR- und TB-*Anwendungsbereiche* hinweg berichtet, jedoch beschreibt nur eine kleine Anzahl von Publikationen diese explizit. Abbildung 9 quantifiziert die Abdeckung nach *Anwendungsbereich* und Subdomäne. ICT weist mit 12 Nennungen die höchste Gesamtaktivität auf, gefolgt von Power Systems (5) und RAN & Mobile Devices (5). IoT/IIoT macht 4 Nennungen aus, während CPS (3) und ICS (3) seltener

auftreten. Intelligent Transportation Systems bleibt mit 2 Nennungen spärlich vertreten. Über die Subdomänen hinweg bleibt Relational Database mit 15 Nennungen am häufigsten, konzentriert in ICT (7) und vertreten in Power Systems (3), ICS (2), CPS (1), IoT/IIoT (1) und Intelligent Transportation Systems (1). NoSQL Database summiert sich auf 9, angeführt von ICT (3) und RAN & Mobile Devices (3), mit weiteren Einträgen in Power Systems (1), IoT/IIoT (1) und Intelligent Transportation Systems (1). Time Series Database tritt 5-mal auf, verteilt auf RAN & Mobile Devices (2) sowie CPS, ICS und Power Systems (je 1). Speicher-Backends jenseits von Datenbanken sind selten. File & Block Storage tritt nur in IoT/IIoT (2) auf. Object Storage wird in ICT (1) und CPS (1) berichtet. Event and Log Storage tritt einmal in ICT (1) auf. Insgesamt zeigt Abbildung 9, dass die Datenspeicherung in CRs und TBs überwiegend auf Datenbanken basiert, wobei relationale Datenbanken am häufigsten und NoSQL-Datenbanken an zweiter Stelle stehen, während andere Speicherkomponenten nur selektiv berichtet werden. In einigen Publikationen wird der primäre Einsatz von Datenbanken als Zielsystem für Cyberangriffe in verschiedenen Szenarien genannt, wie in Kapitel 4.3.1 beschrieben.

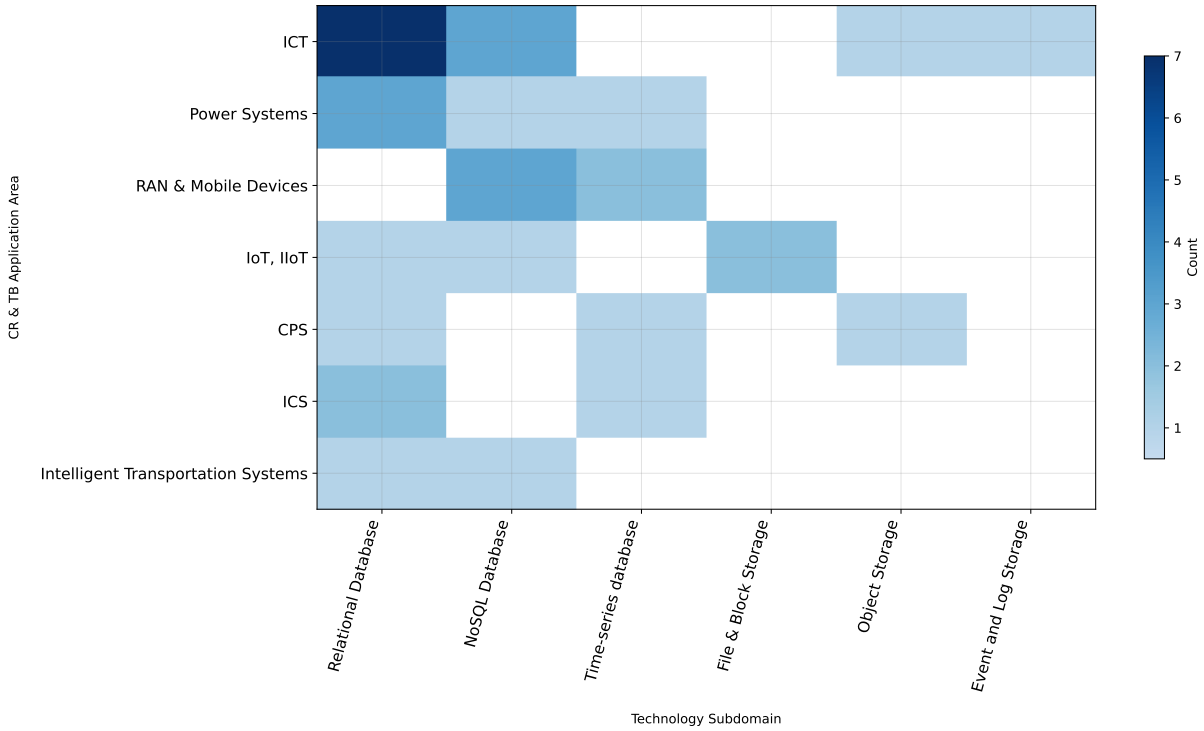


Abbildung 9: Verteilung der Data-Storage-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Relational Database

Ein Smart-Airport-IIoT-Cyber-TB nutzt eine MySQL-Datenbank als relationales Backend zur Langzeitspeicherung gelabelter Netzwerkflüsse und Telemetriedaten und stellt damit die zentrale Datengrundlage für IIoT-Cyber-Twin-Angriffs- und Verteidigungsszenarien in der SAIR-IIoT-Umgebung bereit [84]. Ein Framework zur Generierung von Smart-Grid-CRs nutzt eine MySQL-Datenbank als quelloffenen relationalen Speicher, der virtuelle IEDs mit dem Stromsystemsimulator verbindet. Dies ermöglicht die automatisierte Erstellung und Verwaltung von Smart-Grid-CR-Instanzen auf Basis von Stromsystemmodellen [106]. In einem TB für Information-Environment-Operationen wird PostgreSQL als relationale Datenbank des zentralen Servers eingesetzt und über eine FastAPI-REST-Schnittstelle angebunden. Darüber sind Grafana-Dashboards integriert. PostgreSQL wurde ausgewählt, da es nativ von Grafana unterstützt wird [186]. Das industrielle Steuerungssimulations-Framework ICSSIM nutzt SQLite als gemeinsame relationale

Datenbankdatei zwischen Docker-Containern, sodass simulierte ICS-Komponenten auf gemeinsame Daten zugreifen können. Dies unterstützt integrierte Tests industrieller Steuerungsszenarien [47].

NoSQL Database

Eine Echtzeit-Cybersicherheits-Überwachungsarchitektur für EV-Ökosysteme nutzt MongoDB als Not Only SQL (NoSQL)-Datenbank zur Speicherung von Command-Historien und Telemetriedaten von Ladevorgängen, die von mehreren Simple Network Management Protocol (SNMP)-Agenten erfasst werden. Dies stellt das persistente Backend für die Analyse von EV-Daten und die Erkennung von Cyberangriffen bereit [147]. Ein Framework zur Generierung vollständiger 5G- und 6G-Sicherheitsdatensätze nutzt MongoDB als NoSQL-Speicher für Netzregistrierungsdaten, der von Kernnetzfunktionen abgefragt wird, wenn persistente PDU-Sessions für Angriffsszenarien auf IP-Schicht und im Kernnetz rekonstruiert werden [10]. In einer Sicherheitsstudie zu kooperativem Smart Farming wird eine AWS-NoSQL-Datenbank als Cloud-Datenspeicher für Sensorwerte eingesetzt. Dies ermöglicht Betrieben den Zugriff auf Sensordaten gemäß Autorisierungsrichtlinien und unterstützt das Training und die Evaluierung eines leichtgewichtigen Edge-Convolutional Neural Network (CNN)-Transformer-Modells auf Smart-Farming- und Digital-Twin-Angriffsdatensätzen [133].

Time-series Database

Ein TB für cyber-physische Sicherheit eines mehrstufigen Fertigungssystems nutzt InfluxDB als Time-Series-Datenbank zur Erfassung kontinuierlicher Prozess- und Sensordaten neben traditionellen Cyber-Monitoring-Informationen. Dies stellt einen einheitlichen Echtzeit-Datenspeicher zur Analyse physischer und cyberbezogener Ereignisse in der Fertigungsumgebung bereit [41]. Ein offenes O-RAN-TB mit AI-gestützter Steuerung und Überwachung setzt InfluxDB als Time-Series-Backend für iPerf- und Latenzmessungen ein und speichert Echtzeitmetriken, die die Anomalieerkennung und Leistungsanalyse im Funkzugangsnetz unterstützen [130]. PingThings' Berkeley Tree Database (BTrDB) wird als hochperformante Time-Series-Datenbank im mehrschichtigen Cyber-Power-TB RT-METER eingesetzt und speichert Sensor- und Kommunikationsnetzdaten, sodass Echtzeit-Resilienzanalysen für Stromnetze über physische und Cyber-Schichten hinweg durchgeführt werden können [117].

File and Block Storage

Ein blockchain-basiertes Sicherheitsframework für IoT-Systeme im maritimen Transportwesen nutzt InterPlanetary File System (IPFS) als verteiltes File-and-Block-Storage-System zur Speicherung von Sensordaten, die von Edge-Servern in einer IoT/IIoT-Umgebung erfasst werden [92]. IPFS Kubo wird im selben Framework als Implementierungstool zur Bereitstellung und zum Betrieb dieser IPFS-basierten Speicherschicht eingesetzt und stellt die zugrunde liegende verteilte Speicherinfrastruktur für die erfassten Sensordaten bereit [92].

Object Storage

Eine sichere Edge-Computing-Referenzarchitektur für datengetriebene strukturelle Zustandsüberwachung nutzt AWS Simple Storage Service (S3) als Object-Storage-Dienst für Technical Data Management Streaming (TDMS)-Dateien, wobei Raspberry-Pi-Edge-Geräte Messdaten über AWS IoT Greengrass an S3 zur persistenten Speicherung und späteren Analyse senden [59].

Event and Log Storage
In einem TB für APT wird Elasticsearch als Teil einer Elasticsearch, Logstash, and Kibana (ELK)-basierten Monitoring-Box eingesetzt, die Echtzeitspeicherung, -analyse und -visualisierung von Event-Logs bereitstellt und die Erfassung von Telemetrie aus mehreren APT-Szenarien unterstützt, um Angriffe zu untersuchen und robuste Abwehrmaßnahmen zu entwickeln [175].

Tabelle 2: Top-10-Technologien je Subdomäne für Data Storage. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.3. Monitoring and Analytics

Diese *Technology Domain* umfasst Monitoring- und Analytics-Technologien, die über CRs und TBs hinweg eingesetzt werden. Abbildung 10 quantifiziert die Abdeckung nach Domäne und Subdomäne. ICT weist mit 67 Nennungen die höchste Gesamtaktivität auf, gefolgt von ICS (27), IoT/IIoT (19), Power Systems (17), RAN & Mobile Devices (16), CPS (11) und Intelligent Transportation Systems (6). Über die Subdomänen hinweg führt Analysis & Verification mit 54 Nennungen, gefolgt von Data Collection (43), Log Management (32) und Visualization & Dashboarding (30). Assets Monitoring ist mit nur 4 Nennungen selten. Innerhalb von Analysis & Verification konzentriert sich die Aktivität auf ICT (16) und ICS (11), mit zusätzlicher Nutzung in RAN & Mobile Devices (7), Power Systems (6), Intelligent Transportation Systems (6), CPS (5) und IoT/IIoT (3). Data Collection wird von ICT (15) und IoT/IIoT (11) angeführt, gefolgt von ICS (8), Power Systems (5) sowie CPS und RAN & Mobile Devices (je 2). Log Management wird von ICT (19) dominiert, mit weiteren Einträgen in ICS (5), Power Systems (4) und RAN & Mobile Devices (4). Visualization & Dashboarding erreicht in ICT (15) den Höchstwert und tritt in CPS (4), ICS (3), IoT/IIoT (3), RAN & Mobile Devices (3) und Power Systems (2) auf. Assets Monitoring wird nur in ICT (3) und IoT/IIoT (1) berichtet. Insgesamt werden Monitoring and Analytics in CRs und TBs durch Analyse- und Datenerfassungs-Workflows geprägt, wobei ICT die breiteste und tiefste Abdeckung beisteuert, während Assets-orientiertes Monitoring vergleichsweise selten bleibt.

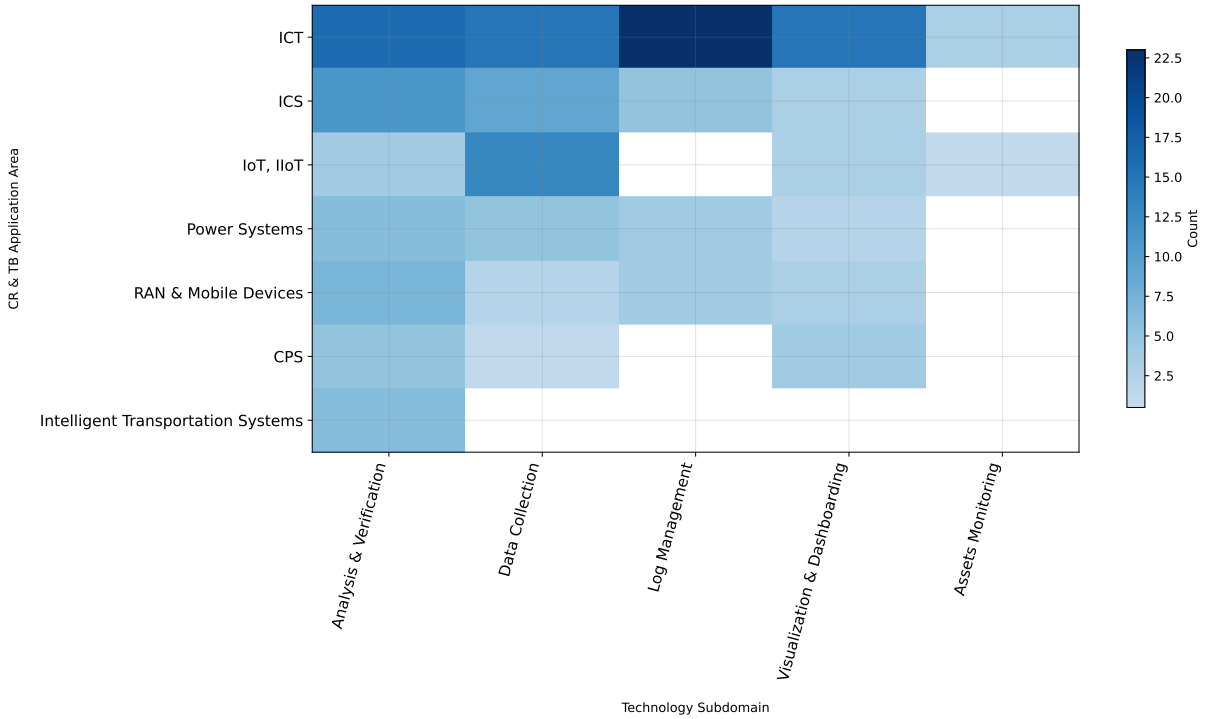


Abbildung 10: Verteilung der Monitoring-and-Analytics-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Analysis and Verification

In einem TB für cyber-physische Sicherheit eines mehrstufigen Fertigungssystems wird Wireshark zur Erfassung und Analyse von Netzwerkverkehr eingesetzt, indem Netzwerkverkehr protokolliert wird. Dies erweitert das Monitoring über traditionelle Cyber-Daten hinaus um Sensordaten neben anderen TB-Komponenten [41]. In einem Penetrationstest-TB für 5G-Systeme wird Wireshark zur Live-Traffic-Erfassung und Feature-Extraktion eingesetzt, indem Traffic auf einzelnen Netzwerksegmenten in simulierten Topologien analysiert wird. Dies unterstützt die Durchführung und Analyse von Angriffen in der entworfenen Umgebung [34]. Eine Modbus-fokussierte SCADA-Sicherheitsstudie nutzt ScadaBR als SCADA-Leitstellen-HMI auf einer dedizierten virtuellen Maschine, wo es mit einem Modbus-Server kommuniziert, um verdeckte SCADA-Hijacking- und Blackout-Angriffsszenarien zu unterstützen, die Protokollschwachstellen ausnutzen [197]. In einer Smart-Grid-Cyber-Range-as-a-Service auf einer OpenStack-Cloud-Plattform fungiert ScadaBR als SCADA-System auf dem Umspannwerks-Host innerhalb einer virtuellen Umgebung, die reale Systeminfrastruktur nachahmt und die automatisierte Instanziierung und Nutzung von Smart-Grid-Cyber-Range-Instanzen unterstützt [35].

Data Collection

Wireshark wird zur Generierung von Netzwerkdatensätzen in einer Sicherheitsstudie zu kooperativem Smart Farming eingesetzt, wo es drahtlose Zugangspunkte überwacht und Traffic aufzeichnet, um Zugangspunkte zu identifizieren und deren Basic Service Set Identifiers (Basic Service Set Identifiers (BSSIDs)) aufzulisten, im Rahmen des Aufbaus von Smart-Farming-Netzwerkdatensätzen für die Bedrohungsanalyse [133]. In einer 5G-Sicherheitsstudie zur HTTP/2-Anomalieerkennung dient Wireshark als Paketerfassungstool im Datenerfassungsprozess und zeichnet HTTP/2-Pakete während des Normalbetriebs des 5G-Netzwerks auf, um Eingabe-Traces für das vorgeschlagene Anomalieerkennungs-Framework bereitzustellen [201]. Tcpdump wird in einem flexiblen hybriden

TB zur Absicherung industrieller Systeme eingesetzt, wo eingehender und ausgehender Rohdatenverkehr erfasst und gespeichert wird, als Teil eines umfassenden Logging-Aufbaus, der alle möglichen Logs aus dem TB sammelt, um die Cyber-Defense-Evaluierung und die anschließende Traffic-Analyse zu unterstützen [43]. In einem substation-fokussierten Cybersicherheitsdatensatz wird Tcpdump eingesetzt, um Netzwerkverkehr über einen Zeitraum von sieben Tagen mittels eingebetteter Software zu erfassen. Dabei werden Paket-Traces gesammelt, die später zum Training von Intrusion-Detection-Systemen auf Basis von Machine-Learning-Modellen für elektrische Umspannwerke verwendet werden [65].

Log Management

In der DefAtt-Architektur virtueller Cyber-Labs für Forschung und Ausbildung wird Elastic Logstash zur Verarbeitung und Filterung von Ereignisdaten eingesetzt, indem übermittelte Events mit Filtern angereichert werden, um sie zu modifizieren oder zu annotieren, während Elasticsearch die Echtzeitsuche und -analyse von Logs bereitstellt, indem die Daten als Dokumente in einem oder mehreren Indizes innerhalb der DefAtt-Umgebung gespeichert werden, die sich auf netzwerkbasierte Angriffe und deren Abwehr konzentriert [104]. Ein TB zur reproduzierbaren und anpassbaren Generierung von Logdaten für Cybersicherheitsexperimente nutzt Elastic Logstash und Elasticsearch gemeinsam zur Speicherung und Suche von Logdaten: Elastic Logstash ist für das Sammeln, Speichern, Durchsuchen und Visualisieren von Logdaten zuständig, und Elasticsearch unterstützt Erfassung, Speicherung, Suche und Visualisierung von Logdaten in einem TB, das zur Generierung realistischer Logdaten für fundierte Cybersicherheitsexperimente konzipiert ist [189].

Visualization & Dashboarding

Ein TB zur Simulation von Sicherheit und Resilienz von Bahninfrastruktur nutzt Grafana als Präsentations-Dashboard, wobei mehrere Analysetools und ein Grafana-basiertes Dashboard entwickelt wurden, um Informationen aus laufenden Experimenten anzuzeigen, einschließlich DDoS-Angriffsszenarien [120]. In einer kooperativen Smart-Farming-Infrastruktur wird Grafana auf jedem Betrieb als Visualisierungstool installiert, um eine intuitivere und detailliertere Darstellung der Sensordaten bereitzustellen, die im effizienten föderierten Transfer-Learning-basierten Anomalieerkennungsaufbau verwendet werden [134]. Ein TB für APT setzt Kibana als Teil einer ELK-basierten Monitoring-Box ein, die Elasticsearch, Logstash und Kibana kombiniert, um Echtzeitspeicherung, -analyse und -visualisierung von Event-Logs aus mehreren APT-Szenarien bereitzustellen [175]. In einem TB, das auf die Generierung realistischer Logdaten für Cybersicherheitsexperimente ausgerichtet ist, wird Kibana auf dem Log-Server als Visualisierungstool eingesetzt, um die generierten Log-Datensätze direkt zu analysieren, bevor sie optional für die Offline-Nutzung exportiert werden [189].

Assets Monitoring

In einer quelloffenen CR, die das Cybersicherheitslernen stärken soll, wird Prometheus als Monitoring-Tool eingesetzt, um zusammen mit Moodle und Grafana Monitoring-Dienste in der Bereitstellung anzubieten. Dies unterstützt verbesserte Lernergebnisse und Monitoring innerhalb der Range [37]. Innerhalb des SEAGuard-Frameworks für IoT-Systeme im maritimen Transportwesen wird Prometheus neben der Blockchain-Plattform eingesetzt, um Leistungsmetriken zu erfassen, die anschließend mit den Monitoring-Komponenten visualisiert werden. Dies ermöglicht die Beobachtung des Verhaltens und der Leistung der vorgeschlagenen Architektur [92].

Tabelle 3: Top-10-Technologien je Subdomäne für Monitoring and Analytics. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.4. Computing Platform

Diese *Technology Domain* umfasst Computing-Plattform-Technologien, die CRs und TBs zugrunde liegen. Abbildung 11 quantifiziert die Abdeckung nach *Anwendungsbereich* und Subdomänen. ICT dominiert insgesamt mit 101 Nennungen, gefolgt von ICS (30), Power Systems (16), IoT/IIoT (14), RAN & Mobile Devices (13), CPS (10) und Intelligent Transportation Systems (6). Über die Subdomänen hinweg sind Cloud Infrastructure (35) und Containerisation (35) gemeinsam am häufigsten vertreten. Es folgen 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) und Infrastructure Instantiation Systems (3). Auf Ebene der *Anwendungsbereiche* konzentriert sich Containerisation auf ICT (13) und ICS (10), mit zusätzlicher Nutzung in RAN & Mobile Devices (6). Cloud Infrastructure wird von ICT (18) angeführt und tritt durchgängig in ICS, Power Systems und IoT/IIoT (je 4) auf. Infrastructure Provisioning and Configuration erreicht in ICT (23) den Höchstwert und tritt in den übrigen *Anwendungsbereichen* nur vereinzelt auf, während es für ICS nicht berichtet wird. Virtualisierungstechnologien werden hauptsächlich für ICT und ICS berichtet, wobei Typ-2-Hypervisoren 12-mal in ICT und 6-mal in ICS sowie Typ-1-Hypervisoren 9-mal in ICT und 6-mal in ICS auftreten. Software Provisioning and Configuration konzentriert sich fast vollständig auf ICT (11) und tritt nur geringfügig in Power Systems (2) auf. Integrated Testbed Solutions sind mit geringen Werten über alle *Anwendungsbereiche* verteilt, und Container Orchestration wird hauptsächlich in ICT (4) und RAN & Mobile Devices (3) berichtet. Insgesamt wird die Abdeckung der Computing Platform durch die ICT-fokussierte Nutzung von Cloud- und containerbasierten Stacks geprägt, unterstützt durch Virtualisierung, während integrierte Lösungen und automatisierte Instanziierungsmechanismen über die *Anwendungsbereiche* hinweg seltener berichtet werden.

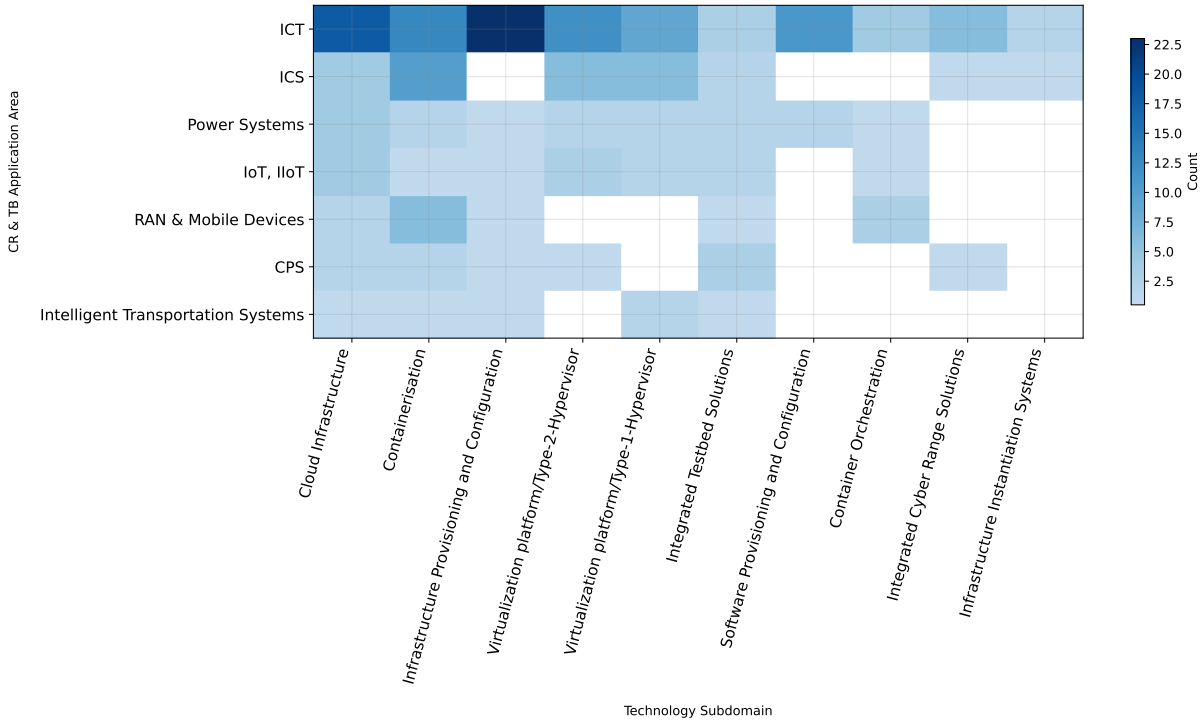


Abbildung 11: Verteilung der Computing-Platform-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Cloud Infrastructures

Ein autonomes Cybersicherheits-TB für OT-Netzwerke nutzt OpenStack als Tool zur dynamischen Steuerung der für die Digital-Twin-Instanziierung benötigten Compute-, Speicher- und Netzwerkressourcen, indem es einen einfach bereitzustellenden OpenStack-basierten Netzwerkemulator bereitstellt, der zum Testen verschiedener Angriffstypen genutzt wird, die zu OT-Anlageninstabilität führen [141]. Eine CR für skalierbare Cybersicherheitsexperimente und -training nutzt OpenStack als Cloud-Computing-Infrastruktur: Die NCL bietet eine Cloud-Computing-Umgebung mit einer Prototypimplementierung auf Basis der OpenStack-Infrastruktur, sodass die CR, eine virtuelle Umgebung, die kritische Infrastruktur nachahmt, auf einer OpenStack-Cloud-Plattform bereitgestellt werden kann [35]. Eine AWS-Elastic Compute Cloud (EC2)-Public-Cloud-CR-Bereitstellung nutzt AWS als Plattform für die Cloud-Bereitstellung der CR und stellt einen Ansatz vor, der Cybersicherheitstrainings in der AWS-Cloud in großem Maßstab und zu relativ geringen Kosten durchführt [19]. Ein IIoT-Sicherheits-TB zur Bewertung und Minderung von Netzwerkschwachstellen nutzt AWS als Cloud-IoT-Infrastruktur, wobei Sensoren mit unterschiedlichen Protokollen Daten über Monitoring-Gateways senden, die die Daten über eine DMZ an die AWS-Cloud weiterleiten, um betriebliche und cybersicherheitsrelevante Risiken im Zusammenhang mit IIoT-Bereitstellungen zu untersuchen [75].

Containerisation

Ein cyber-physisches Fuzzing-Framework für Unmanned Aerial Vehicle (UAV)-Systeme konfiguriert seine Simulationsumgebung auf einem Ubuntu-Linux-Host, auf dem Docker die containerisierte Laufzeitumgebung für die Flugverhaltenssimulationen bereitstellt, die für Butterfly-Effekt-Phänomene im UAV-Regelkreis ausgeführt und analysiert werden [90]. Im ICSSIM-Framework zum Aufbau von ICS-Sicherheits-TBs wird jede ICS-Komponente innerhalb eines isolierten Docker-Containers simuliert, sodass Module beim Aufbau individueller ICS-Sicherheitsexperimente flexibel kombiniert, erweitert oder ersetzt werden können [47]. Das virtuelle maritime TB MaCySTe,

das die Netzwerkinfrastruktur und zentrale Komponenten bordseitiger cyber-physischer Systeme für realistische Cybersicherheitstests und -trainings mit maritimem Personal nachbildet, startet jedes Trainingsszenario über Shell-Skripte, die auf Podman zurückgreifen, um Container-Netzwerke zu erstellen und Pods sowie Flatpak-basierte Anwendungen auszuführen [99].

Infrastructure Provisioning and Configuration

Eine groß angelegte CR für Cybersicherheitstraining nutzt Terraform als Infrastructure-as-Code-Workflow-Engine zusammen mit VMware vSphere, um Virtual Machine (VM)-Templates zu erstellen und zu speichern, einschließlich Komponenten wie Active Directory, Domain Name System (DNS) und Domänencontrollern. Dies ermöglicht die vielseitige Bereitstellung der Range-Infrastruktur mit minimalem manuellem Aufwand [127]. In der akademischen CR Tectonic wird Terraform für die automatisierte Infrastrukturbereitstellung eingesetzt, indem die zu instanziierenden Ressourcen und anzuwendenden Konfigurationen definiert werden, während Libvirt On-Premises-Virtualisierung bereitstellt, mit der Lehrende Systeme und Netzwerke für die Trainingsszenarien bereitstellen [64]. Für die CryptoGuard-Studie zu Cryptojacking wird Libvirt eingesetzt, um mehrere VMs auf einem Host zu betreiben und so das TB zur Datenerfassung aufzubauen. Dies ermöglicht die Durchführung von Experimenten auf mehreren VMs unter einem gemeinsamen Setup [131]. In der CyberExpert-Plattform für erfahrungsbasiertes Lernen dient Libvirt als Virtualisierungs-API, die Tools wie Foreman und Guacamole zur Steuerung und zum Starten von VMs nutzen. Dies unterstützt eine virtuelle und praxisnahe CR-Umgebung für höherstufiges Cybersicherheitstraining [66].

Virtualization Platform/Type-2-Hypervisor

Eine virtuelle Cyber-Lab-Plattform für netzwerkbasiertes Angriffs- und Verteidigungstraining nutzt VirtualBox als Virtualisierungsplattform (Typ-2-Hypervisor), um Rechner in einer vernetzten Umgebung als VMs zu simulieren. Dies ermöglicht die kostengünstige Erstellung und Bereitstellung von CR-Lab-Umgebungen für Ausbildung und Forschung [104]. In einem Smart-Grid-Cybersicherheits-TB wird VirtualBox für die Simulation von Umspannwerk und Leitstelle eingesetzt, indem VMs betrieben werden, die die Hardware an beiden Standorten nachbilden, wobei das virtualisierte Netzwerk über eine Router-VM verbunden ist, um die Smart-Grid-Kommunikationsumgebung zu emulieren [215]. Eine ICS-CR für Sicherheitstraining basiert auf VMware Workstation als Virtualisierungsplattform, die alle VMs verwaltet und Operationen wie Start, Pausierung und Herunterfahren der in den Trainingsszenarien verwendeten Betriebssysteme steuert [100]. Das digital-forensische TB IoT-CAD setzt VMware Workstation ein, um die VMs in der Anwendungsschicht zu hosten, einschließlich einer Kali-Linux-VM, die als offensives System agiert, um Angriffe gegen IoT-Geräte und -Dienste für Experimente zur Cyberangriffsattribution auszuführen [110].

Virtualization Platform/Type-1-Hypervisor

Eine Studie zu zeitbasierter Migration virtueller Maschinen als Moving-Target-Defense gegen hostbasierte Angriffe modelliert Angreifer- und Opferrechner als VMs, die auf dem Kernel-based Virtual Machine (KVM)-Hypervisor laufen, wobei beide VMs Ubuntu Server 20.04.2 mit Kernel 5.4.0-72 und KVM 4.2.1 nutzen, sodass KVM die Verwaltungsschicht für virtuelle Maschinen in der auf Stochastischen Petrinetzen basierenden Evaluierungsumgebung bereitstellt [184]. Im PenGym-Framework zum Training von Reinforcement-Learning-Penetrationstest-Agenten wird KVM zur Verwaltung virtueller Maschinen eingesetzt, als Virtualisierungstechnologie, die der CR zugrunde liegt. Dies ermöglicht die Erstellung von VMs mit vordefinierten Diensten und Prozessen als Teil der Netzwerkumgebung für realistisches Agenten-Training [122]. Eine groß angelegte CR für Cybersicherheitstraining nutzt VMware vSphere als Computing-Plattform, um VM-Templates zu erstellen und zu speichern, wobei vSphere zum Erstellen und Verwalten von Templates eingesetzt

wird, die Komponenten wie Active Directory, DNS und Domänencontroller als Teil einer flexiblen Trainingsinfrastruktur umfassen [127]. In einer Echtzeit-Monitoring-Architektur für verbesserte Cybersicherheit im EV-Ökosystem wird vSphere als Computing-Plattform beschrieben, die zur Verwaltung und Bereitstellung der VMs eingesetzt wird, welche die Komponenten des EV-Monitoring-Frameworks hosten. Dies unterstützt die Erfassung und Analyse von Daten aus unterschiedlichen Elementen des EV-Ökosystems [147].

Integrated Testbed Solutions

Ein Echtzeit-Simulations-TB für cyber-physische Großstromsysteme nutzt EXata CPS (Cyber-Physical Network Simulator), um das Cyber-Netzwerk zu simulieren: Die EXata-Netzwerkmodellierung wird eingesetzt, um das Cyber-System zu modellieren und mit der Echtzeit-Netzwerkemulation zu interagieren, die auf dem EXata-Server läuft, während Echtzeitsimulatoren von OPAL-RT und RTDS die Stromnetze simulieren [124]. Ein experimentelles TB zu Sicherheits- und Stabilitätsherausforderungen bei wechselrichterbasierten Solar-Verteilerzeugungssystemen integriert EXata CPS als Cyber-Netzwerk-Simulationssoftware zur Simulation des Cyber-Netzwerks. Dies unterstützt verschiedene Industrieprotokolle und -technologien und ermöglicht die Simulation komplexer Netzwerkszenarien, deren Schwachstellen und potenzielle Auswirkungen analysiert werden [116]. Aerial Experimentation and Research Platform for Advanced Wireless (AERPAW) wird als Droneninfrastruktur in einem TB eingesetzt, das Optimierungsmethoden für federated-learning-gestützte Netzwerk-Incident-Anomalieerkennung in Drohnenschwärmen untersucht. Dabei werden Abwehrmechanismen wie Differential Privacy und Adversarial Training evaluiert sowie Genauigkeits-, System- und Netzwerknutzungsmetriken unter Testfällen einschließlich gutartiger, leicht vergifteter, stark bösartiger und sicherer Situationen erfasst [85].

Software Provisioning and Configuration

In einer groß angelegten CR für Cybersicherheitstraining wird Ansible als Konfigurationsmanagement-Engine für die Software-Bereitstellung eingesetzt und unterstützt die vielseitige und flexible Bereitstellung der Range-Infrastruktur mit minimalem manuellem Aufwand [127]. Eine cloudbasierte Smart-Grid-CR für skalierbare Cybersicherheitsexperimente und -training nutzt Ansible auf dem Controller-Host, um die Bereitstellung von Controller- und Umspannwerksknoten als Teil der virtuellen Umgebung auf einer OpenStack-Cloud-Plattform zu automatisieren [35]. In Arbeiten zu APT-Szenarien für CRs wird AWX als Verwaltungssoftware für die Administration und Orchestrierung von APT-Szenarien eingesetzt, wobei eine graphbasierte Logik-Engine für APT-Szenarien in Kombination mit AWX in vollständig virtualisierten CRs betrieben wird [21].

Container Orchestration

Ein Cryptojacking-Abwehr-Framework für Linux-Cloud-Umgebungen nutzt Kubernetes für die Container-Orchestrierung, indem der CryptoGuard-Agent als DaemonSet bereitgestellt wird, sodass auf jedem Knoten ein Monitoring-Pod läuft und Syscall-Daten über den gesamten Cluster hinweg erfasst werden kann [131]. In einem 5G-Kernnetz-Anomalieerkennungsaufbau werden alle 5G-Kernnetzfunktionen als Kubernetes-Pods mithilfe von Helm-Charts aus einem öffentlichen Repository bereitgestellt, sodass das 5GCGuard-Framework auf einer Kubernetes-verwalteten 5G-Kernnetzumgebung zur Evaluierung der Anomalieerkennung läuft [178]. Eine Raspberry-Pi-basierte CR für Web-Angriffstraining nutzt Docker Swarm als Container-Orchestrierungsplattform, um neue Container automatisch zum Lastausgleich über unterschiedliche Clusterknoten zu verteilen und die Clusterknoten drahtlos zu verwalten [126]. In einer Smart-Grid-Cyber-Range-as-a-Service erstellt ein Bereitstellungstool Docker-Images auf jedem Knoten und startet Docker-Swarm-Overlay-Netzwerke, sodass die CR, realisiert als virtuelle Umgebung auf einer OpenStack-Cloud-Plattform, Container über die teilnehmenden Knoten hinweg orchestrieren kann [35].

Integrated Cyber Range Solutions

Eine Studie zum Vergleich reproduzierter Cyber-Experimente über unterschiedliche Emulations-TBs hinweg nutzt Minimega als emulationsbasiertes Cyber-TB, wobei ein mathematisches Modell gegen Experimente mithilfe der Minimega-Emulation validiert wird und Erkenntnisse zur Reproduzierbarkeit der ursprünglichen Experimente sowie zur Erkennung von gegnerischem Netzwerkscanning mittels Emulation gewonnen werden [179]. In Arbeiten zur Verifikation von Cyber-Emulationsexperimenten anhand von Metriken virtueller Maschinen und Hosts wird Minimega als Emulationsplattform eingesetzt: Das Framework instanziiert Minimega, um die CRX Iceberg zu evaluieren und die Bewertung von Übungen in dieser emulationsbasierten Umgebung zu unterstützen [182]. Der Netzwerk-Intrusion-Datensatz GeNIS wird mithilfe der cloudbasierten Netzwerksimulationsinfrastruktur entwickelt, die GECAD auf der Plattform Airbus CyberRange zur Verfügung steht. Die Plattform stellt dabei die Ressourcen zur Generierung von Traffic und rohen Netzwerkpaketen in einer Unternehmenstopologie bereit, die bösartige Flows von Angreifern, gutartigen Traffic legitimer Nutzender und Hintergrundverkehr eines Unternehmensnetzwerks umfasst [167].

Infrastructure Instantiation Systems

Eine CR-Plattform für Training nutzt Naumachia als Infrastructure-Instantiation-System zur Infrastrukturbereitstellung und -konfiguration. Naumachia wird als Docker-Netzwerk beschrieben, das jeder Challenge eine isolierte Umgebung bereitstellt, die als eigenständiger Docker-Container bereitgestellt wird, innerhalb einer aus quelloffenen Tools aufgebauten Plattform für Themen wie Snort-Regelerstellung, forensische Analyse und Man-in-the-Middle-Spoofing [193]. Eine cloudbasierte CR-Bereitstellung erweitert die Funktionalität des CR-Instanziierungssystems Cyber Range Instantiation System (CyRIS), das als Open Source auf GitHub verfügbar ist, um einen Ansatz umzusetzen, der die AWS-EC2-Public-Cloud-Plattform nutzt, um Cybersicherheitstrainings in großem Maßstab und zu relativ geringen Kosten durchzuführen [19]. Im PenGym-Framework zum Training von Penetrationstest-Agenten stellt CyRIS einen automatischen CR-Erstellungsmechanismus bereit. Das Action/State-Modul fungiert als Schnittstelle zwischen Agenten und Umgebung, und dieser automatische CR-Erstellungsmechanismus wird in PenGym integriert, indem CyRIS genutzt wird, um die Erstellung der Netzwerkumgebung und gute Ausführungsleistung zu unterstützen [122].

Tabelle 4: Top-10-Technologien je Subdomäne für Computing Platform. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.5. Custom Development

Diese *Technology Domain* umfasst Custom-Development-Technologien, die in CRs und TBs eingesetzt werden. Abbildung 12 zeigt die Abdeckung nach *Anwendungsbereich* und *Technology Subdomain*. ICT konzentriert die meiste Aktivität mit 70 Nennungen, gefolgt von IoT, IIoT (21), CPS (16), ICS (14) und RAN & Mobile Devices (14), Power Systems (6) und Intelligent

Transportation Systems (2). Über die Subdomänen hinweg führt AI & ML mit 55 Nennungen, dominiert von ICT (34) und ergänzt durch CPS (9) und RAN & Mobile Devices (8). Dataset Generation folgt mit 36 Nennungen, getrieben von IoT, IIoT (15) und ICT (13), mit zusätzlicher Nutzung in Power Systems (3) und RAN & Mobile Devices (3) sowie Einzeleinträgen in CPS (1) und ICS (1). Data Science summiert sich auf 13 und wird hauptsächlich in ICT (8), ICS (3) und IoT, IIoT (2) berichtet. Integrated Development Environment tritt 11-mal auf, angeführt von ICT (5) und ICS (3), mit kleineren Beiträgen in CPS (2) und IoT, IIoT (1). Die übrigen Subdomänen sind spärlich vertreten, wobei Backend Frameworks (8), Build-Toolchain (4) und Visualization & Dashboarding (4) die wichtigsten sekundären Kategorien darstellen. Infrastructure, Middleware, Reverse Engineering and Binary Analysis, Runtime Environment und Simulation Environment treten jeweils nur einmal auf. Insgesamt zeigt die Heatmap, dass Custom Development in ICT stark datenzentriert ist, wobei IoT, IIoT erheblich zur Dataset-Generation beiträgt. CPS und RAN & Mobile Devices weisen eine nennenswerte Nutzung von AI und ML auf, jedoch mit geringerer Breite, während sich die Aktivität in ICS stärker auf IDEs, Visualisierung und Data Science konzentriert. Andere Domänen zeigen isolierte, domänenspezifische Einzelfälle.

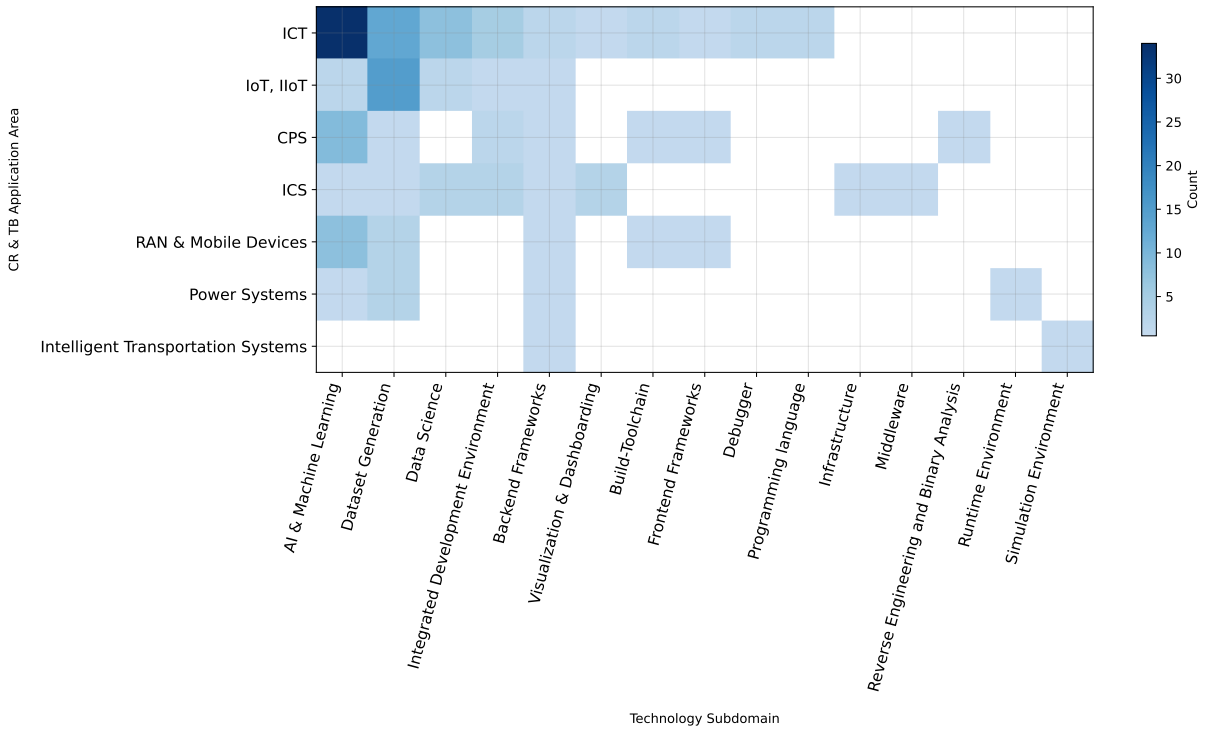


Abbildung 12: Verteilung der Custom-Development-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

AI & Machine Learning

Ein SDN-gesteuertes IoT-TB zur DDoS-Angriffserkennung nutzt TensorFlow als Machine-Learning-Framework und Keras als unterstützende Bibliothek für die AI- und ML-Anwendungsentwicklung. Die Trainingsdatensätze werden getrennt vom Rohverkehr erfasst, und Modelle werden mit unterschiedlichen Parametern trainiert, deren Ergebnisse verglichen und dargestellt werden, um einen effizienten Ansatz zur DDoS-Erkennung auf der Kernschicht des SDN-gesteuerten TB zu evaluieren [78]. In der 5G-CR SPIDER fungiert TensorFlow erneut als Machine-Learning-Framework und Keras als Machine-Learning-Bibliothek, beide als Data-Science-Tools genutzt, um ML-Komponenten zu entwickeln, die anschließend in die CR überführt werden. Diese ML-Tools unterstützen Szenarien in einer 5G-fokussierten Range, die für komplexe Cyberangriffsszenarien und die Bewertung von Cyberrisiken konzipiert ist [146].

Dataset Generation

In einer Arbeit zu einer SDN-basierten Umgebung wird Comma-Separated Values (CSV) als Datenformat verwendet, in dem Mittelwert- und Standardabweichungswerte gespeichert werden, die während der Datenvorverarbeitung ermittelt wurden. Dies ermöglicht die Normalisierung und Bereitstellung von Features für das anschließende Modelltraining. Im selben Setting wird die DPKT-Python-Bibliothek zur Datenverarbeitung und Flow-Feature-Berechnung eingesetzt. Die Datensatzanbietenden stellen Code bereit, der die Flow-Features mithilfe von DPKT als Teil der Dataset-Generation-Pipeline berechnet [143]. In einer Studie, die einen umfassenden Datensatz zu Substation-Traffic für Cybersicherheitsanwendungen in Umspannwerken vorstellt, wird CSV als Datenformat für Netzwerkfeatures eingesetzt, wobei zwei Arten von Dateien zum Datensatz hinzugefügt werden: eine mit traffic-bezogenen Informationen und eine weitere mit einer ausgewählten Menge relevanter Features [65].

Data Science

In einer Arbeit zu dynamischer und zuverlässiger Intrusion Detection gehören NumPy und Pandas zur Data-Science-Subdomäne und werden zur Feature-Extraktion innerhalb der Datenverarbeitungs-Pipeline eingesetzt, was den Intrusion-Detection-Ansatz unterstützt, der auf eine höhere Robustheit des Systems gegenüber motivierten Angreifenden abzielt [45]. In einer weiteren Studie werden NumPy und Pandas als Teil des Python-basierten experimentellen Aufbaus für Data-Science-Aufgaben eingesetzt, wo sie das Datenmanagement übernehmen, das Modelltraining unterstützen und die Implementierung von Graphalgorithmen ermöglichen. Damit bilden sie einen Kernbestandteil der Data-Science-Toolchain, die zur Evaluierung der vorgeschlagenen Methode gegen die betrachteten Angriffe eingesetzt wird [142].

Integrated Development Environment

In einem ICS-fokussierten, modularen und quelloffenen Framework zur Bewertung der Sicherheit von SCADA-Systemen wird FUXA als integrierte Entwicklungsumgebung für die HMI-Entwicklung eingesetzt, wobei die HMI-Komponente des TB durch das SCADA/HMI-Framework FUXA als Teil der Target-Infrastructure-Layer implementiert wird, die die Untersuchung heterogener Angriffsszenarien und Sicherheitsmethodiken innerhalb der SCADA-Umgebung unterstützt [44]. In einem ICT-Cybersicherheits-TB, das Keylogger untersucht, wird Jupyter Notebook als integrierte Entwicklungsumgebung für die Keylogger-Entwicklung und Datenvisualisierung eingesetzt, wobei das Notebook zum Schreiben des Codes für das Keylogger-Programm und zur Unterstützung der Visualisierung keyloggerbezogener Daten genutzt wird, als Teil der Demonstration zentraler Funktionen eines wirksamen Cybersicherheits-TB [20]. In einer weiteren ICT-Umgebung, die den TestCloudIDS-Datensatz und das SparkShield-IDS-Modell vorstellt, dient Jupyter Notebook als Schnittstelle innerhalb eines Anaconda-basierten Setups, wobei PySpark- und FindSpark-Pakete installiert werden und das Notebook als integrierte Umgebung zur Konfiguration und Ausführung des SparkShield-Intrusion-Detection-Modells auf dem TestCloudIDS-Datensatz dient [192].

Backend Frameworks

Eine CR-Übungsplattform nutzt Flask als Backend-Framework zur Implementierung der REST-API eines Learning Management System (LMS), wobei ein VueJS-basiertes LMS über diese Flask-API mit der zugrunde liegenden Docker-Infrastruktur als Teil einer Incident-Response-CR-Übung verbunden ist [60]. In einer Smart-Grid-Cyber-Range-as-a-Service stellt Flask die Webanwendung auf dem Controller-Host bereit, die als Graphical User Interface (GUI) für die Range fungiert, welche als virtuelle Umgebung auf einer OpenStack-Cloud-Plattform beschrieben wird [35]. Für einen datenschutzwahrenden Widerrufsmechanismus auf Blockchain-Basis im

Bereich intelligenter Verkehrssysteme wird Node.js als Backend-Framework für eine Blockchain-Simulationsumgebung eingesetzt, die den vorgeschlagenen Widerrufsmechanismus unterstützt und darauf abzielt, die Prüfzeit zu reduzieren sowie die Abhängigkeit von einer zentralen Behörde zu beseitigen [160]. In einer dockerisierten Android-Plattform für mobile Cyber-Range-Szenarien implementiert das in Node.js geschriebene Backend-Modul eine erweiterbare Schnittstelle, die Aktionen wie den Versand einer bösartigen SMS oder E-Mail steuert, um Phishing-Angriffe innerhalb des mobilgeräte-fokussierten Cyber-Range-Frameworks zu simulieren [30].

Visualization & Dashboarding

In einem ICS-TB für resiliente Betriebssysteme wird Ignition SCADA in der Visualization-and-Dashboarding-Subdomäne eingesetzt, um die SCADA-Benutzeroberfläche zu entwickeln. Dabei werden industrielle Netzwerkumgebungen nachgebildet und SCADA-Visualisierung für OT-Protokolle wie ModbusTCP und DNP3 innerhalb einer virtuellen Infrastruktur bereitgestellt, die an einen Typhoon-HIL-Echtzeitsimulator gekoppelt ist [174]. In einem ICS-Cyber-Defense-Evaluierungs-TB wird Node-RED in der Visualization-and-Dashboarding-Subdomäne als HMI-Umgebung eingesetzt, wobei ein flussbasierter Programmieransatz genutzt wird, um die Mensch-Maschine-Schnittstelle in einem flexiblen hybriden/virtuellen TB aufzubauen, das Cyber-Defense-Evaluierung und umfassende Log-Erfassung aus dem TB unterstützt [43].

Build-Toolchain

Im virtuellen TB MaCySTe für maritime Cybersicherheit ist GNU Make Teil der Build-Toolchain und wird zur Automatisierung von Aufgaben im TB eingesetzt, wobei die Ausführung von Komponenten und Operationen innerhalb der Umgebung verwaltet wird [99]. Innerhalb des NDIF-Frameworks für In-Network-Anwendungen auf Basis neuronaler Netze in einer ICT-Umgebung wird der P4-Compiler in der Build-Toolchain eingesetzt, um P4-Programme zu kompilieren, die die vom Framework benötigte In-Network-Verarbeitungslogik implementieren [95].

Frontend Frameworks

In einer Arbeit, die eine CRX für Incident Response vorstellt, wird VueJS für die Frontend-Entwicklung des LMS eingesetzt, wobei das LMS über eine mit Flask implementierte REST-API mit der zugrunde liegenden Docker-Infrastruktur kommuniziert und die Web-Oberfläche für die Incident-Response-Umgebung bereitstellt [60]. In einer Studie, die dockerisierte Cyber-Range-Komponenten für mobile Geräte in Cyber-Ranges der nächsten Generation vorschlägt, wird React.js zur Implementierung der Benutzeroberfläche eingesetzt, wobei aktuelle Funktionen zusammen mit TypeScript genutzt werden, um kohäsive und lose gekoppelte Frontend-Komponenten für die Interaktion mit der Range-Umgebung zu erstellen [30].

Debugger

In einer ICT-Ausbildungsumgebung, die CTF-artige Übungen einsetzt, sind Gdb und Gef Teil der Debugger-Toolchain für die Sicherheitsübungsumgebung. Umfangreiches Tooling wird bereitgestellt, sodass Studierende mithilfe dieser Debugger zusammen mit vielen weiteren Tools an Challenges arbeiten können, in Szenarien, die CTF, CTFd, Linux-Nutzung, Shell-Scripting, Netzwerksicherheit, Web, Kernel-Sicherheit und Microarchitecture-Speculative-Execution-Angriffe innerhalb derselben Umgebung abdecken [121].

Programming Language

In einer ICT-CR für Cybersicherheitsübungen wird Datalog als Programmiersprache für die formale Szenariomodellierung eingesetzt. Sie liefert eine formale Darstellung von Übungsszenarien

und unterstützt die Verifikation unterschiedlicher Szenarioeigenschaften. Dies wird innerhalb eines Systems umgesetzt, das viele Aufgaben von Cyber-Übungen automatisiert, um Autonomie und Kompetenzentwicklung der Teilnehmenden in der Range-Umgebung zu unterstützen [207]. In einer ICT-CR, die Cyber-Angriffs- und Verteidigungsagenten einsetzt, wird Datalog als Programmiersprache für die formale Modellierung von Agentenentscheidungen eingesetzt. Dabei wird die Entscheidungslogik der Agenten spezifiziert und das Schlussfolgern über Entscheidungseigenschaften ermöglicht, etwa ob das Ziel innerhalb des agentenbasierten Systems erfüllt wird, das Cyberangriffe und -verteidigung in der Range emuliert [208].

Infrastructure

Im modularen, quelloffenen Framework SCASS zur Bewertung der Sicherheit von SCADA-Systemen wird Node-RED im SCADA-System-Container auf der Infrastrukturschicht eingesetzt. Dort realisiert es SCADA-Prozesslogik und HMI-Funktionalität. Innerhalb dieses ICS-TB wird Node-RED als Programmier-Tool genutzt, um industrielle Prozesse zu modellieren und die Gestaltung sowie Ausführung heterogener Angriffsszenarien und Sicherheitsmethodiken gegen die emulierte SCADA-Umgebung zu unterstützen [44].

Middleware

In einer ICS-Cybersicherheitsausbildungs- und Gamification-Umgebung wird OpenMUC als Middleware auf der Target-Infrastructure-Layer eingesetzt, um industrielle Prozessüberwachung und -steuerung bereitzustellen, was die Überwachung und Steuerung industrieller Komponenten und Prozesse innerhalb des TB ermöglicht [87].

Reverse Engineering and Binary Analysis

In einem CPS-Sicherheitsszenario mit gemischter zeit- und ereignisgesteuerter Moving-Target-Defense wird Binary Ninja innerhalb der Subdomäne Reverse Engineering and Binary Analysis eingesetzt, um Binärdateien in LLVM-Bitcode zu übersetzen. Dies stellt Binär-Disassemblierung und Kontrollflussrekonstruktion als Teil der Analyse-Pipeline bereit [132].

Runtime Environment

In einer Stromsystem-CR, die eine Smart-Grid-Konfiguration auf einer OpenStack-Cloud-Plattform nachahmt, wird Open Java Development Kit (OpenJDK) 8 als Laufzeitumgebung innerhalb eines Controller-Containers eingesetzt und stellt die Java-basierten Tools bereit, die für die Ausführung der Controller-Funktionalität sowie zur Unterstützung automatisierter Cybersicherheitsexperimente und -trainings innerhalb der virtuellen Umgebung erforderlich sind [35].

Simulation Environment

In einer Umgebung für intelligente Verkehrssysteme, die einen datenschutzwahrenden Widerrufsmechanismus für Vehicular Ad Hoc Networks (VANETs) mit einer Blockchain unter Verwendung von Akkumulatoren vorschlägt, wird cpprestsdk in der Simulation Environment auf dem Target-Infrastructure-Layer als REST-API-Bibliothek eingesetzt, um die VANET-Infrastruktur mit der REST-API von Hyperledger Composer zu integrieren. Dies ermöglicht die Kommunikation zwischen der VANET-Infrastruktur und den blockchain-basierten Widerrufskomponenten innerhalb des TB [160].

Tabelle 5: Top-10-Technologien je Subdomäne für Custom Development. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.6. Blue Team Operations

Diese *Technology Domain* umfasst Blue-Team-Technologien, die über CRs und TBs hinweg eingesetzt werden. Abbildung 13 quantifiziert die Abdeckung nach *Anwendungsbereich* und Subdomäne. ICT weist mit 46 Nennungen die höchste Gesamtaktivität auf, gefolgt von ICS (30), RAN & Mobile Devices (11), Power Systems (9), CPS (6), IoT/IIoT (6) und Intelligent Transportation Systems (1). Über die Subdomänen hinweg führt Intrusion Detection & Prevention (IDS/IPS) mit 27 Nennungen. Security Information and Event Management (SIEM) & Security Analytics und Vulnerability Management folgen mit jeweils 23 Nennungen. Network Analysis & Reconnaissance summiert sich auf 11, während die übrigen Subdomänen geringere Abdeckung zeigen, darunter Firewalls & Network Security Gateways (5), Training and Practice Systems (4), Malware Analysis (3) und Threat Intelligence (3). Endpoint Detection & Response (Endpoint

Detection and Response (EDR)), Phishing and Social Engineering sowie Reverse Engineering and Binary Analysis treten jeweils 2-mal auf, während Application Security Testing, Deception & Honeypot Systems, Incident Management & Response und Security Hardening jeweils nur einmal vorkommen. Auf Ebene der *Anwendungsbereiche* ist IDS/IPS in ICS (10) und ICT (9) am stärksten vertreten, mit zusätzlicher Nutzung in Power Systems (7) und IoT/IIoT (1). SIEM & Security Analytics konzentriert sich auf ICT (13) und ICS (6), mit weiterer Aktivität in IoT/IIoT (3) und CPS (1). Vulnerability Management ist breit vertreten und wird von ICT (8), RAN & Mobile Devices (7) und CPS (5) getragen, mit Einzeleinträgen in ICS, IoT/IIoT und Intelligent Transportation Systems (je 1). Network Analysis & Reconnaissance konzentriert sich stark auf ICS (8) und tritt nur geringfügig in ICT, IoT/IIoT und RAN & Mobile Devices (je 1) auf. Insgesamt deutet die Heatmap auf einen Defensiv-Stack hin, der auf Erkennung und Telemetrie ausgerichtet ist, wobei IDS/IPS und SIEM als primäre Komponenten dominieren. Dieser Stack wird durch Vulnerability Management und gezielte Analysen ergänzt, wobei ICT und ICS die breiteste und tiefste Abdeckung bieten.

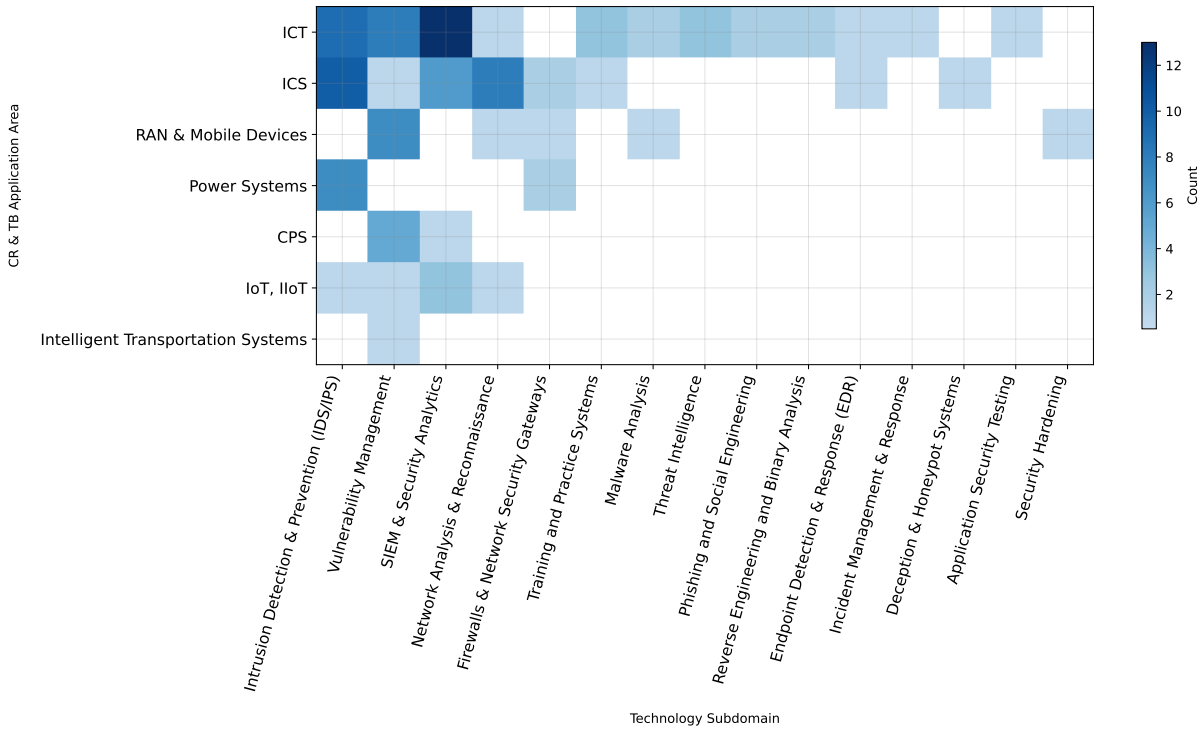


Abbildung 13: Verteilung der Blue-Team-Operations-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Intrusion Detection & Prevention (IDS/IPS)

In einer ICS-Emulationsumgebung (RESlab) wird Snort zur Erkennung von Scanning-Versuchen konfiguriert, wobei die Skripte für jedes Nmap-Portscan-Experiment Snort starten, um verdächtige Ports und Angriffsmuster zu identifizieren, als Teil der Bewertung der Reproduzierbarkeit der Erkennung gegnerischen Netzwerkscannings innerhalb des Labs [179]. Ein weiteres ICS-TB setzt Snort v3.0 mit snort3-Community-Regeln als signaturbasiertes Network Intrusion Detection System (NIDS) ein, das bekannte Angriffsmuster erkennt und die zentrale Intrusion-Detection-Komponente in einem dynamischen und zuverlässigen IDS-Ansatz bildet, der die Robustheit gegenüber motivierten Angreifenden innerhalb der industriellen Steuerungsumgebung erhöhen soll [45]. In einem ICS-TB, das eine kontrollierte und reproduzierbare Umgebung für einen WWTP-Industrieprozess schaffen soll, wird Suricata als primäres Tool zur Erkennung von Netzwerkbedrohungen eingesetzt, das Traffic analysiert, um bösartige von normaler Aktivität zu

unterscheiden und so die Sicherheitsbewertung des Industrieprozesses zu unterstützen [101]. In einem ICT-Umfeld, das eine graphbasierte Analyse von Cyberangriffen vorstellt, werden Suricata-Kommunikationsalarme mit ATT&CK-Alarmen und weiteren Log-Ereignissen kombiniert, um Evidenzpfade zu konstruieren und einen Kill-Chain-Angriffsgraphen aufzubauen, sodass die Suricata-Alarme zu Schlüsselelementen bei der Korrelation erkannter Ereignisse und der Bewertung des Angriffsschweregrads innerhalb des TB werden [153].

SIEM & Security Analytics

In einem ICS-TB, das eine kontrollierte und reproduzierbare virtuelle Umgebung für einen WWTP-Industrieprozess schaffen soll, wird Security Onion für Netzwerk- und Systemüberwachung eingesetzt und als Security-Information-and-Event-Management-Plattform innerhalb der mehrschichtigen Architektur genutzt [101]. In einem Smart-Airport-Cybertwins-Sicherheits-TB für IIoT-Umgebungen stellt Security Onion Netzwerksicherheitsüberwachung, Datenerfassung und Intrusion Detection bereit, wobei eine Tap-Maschine Netzwerkverkehr aufzeichnet und die erfassten Daten über ein dediziertes Datenmanagement-Tool verwaltet werden, als Teil der Evaluierung von Angriffs- und Verteidigungsszenarien [84]. Innerhalb einer Krisenmanagement-Übung, die Cybersicherheitsfachkräfte in der Entscheidungsfindung schult, wird Wazuh SIEM installiert, um Netzwerke und Endpunkte zu überwachen, wobei dessen Schnittstelle genutzt wird, um zu bestätigen, dass während der Übung Traffic erzeugt und beobachtet wurde, als Teil der szenariobasierten Evaluierung [150]. In einem TB, das CyberAlly vorstellt, einen wissensgraphgestützten AI-Assistenten für die Cyberabwehr, stellt Wazuh SIEM das Alert-Monitoring bereit, wobei Teilnehmende beobachten, wie Wazuh Alarme postet, die anschließend von CyberAlly korreliert, gefiltert und analysiert werden, um die Untersuchung von Vorfällen und die Empfehlung von Abwehrmaßnahmen zu unterstützen [81].

Vulnerability Management

In einer Studie, die Tools der nächsten Generation zur Entwicklung von Cybersicherheitsanwendungen vorstellt, wird Nessus für Remote-Vulnerability-Scanning eingesetzt. Nikto ist Teil des defensiven Tool-Sets. Jede Anwendung in dieser Umgebung bietet entweder Angriffs- (Red-Teaming) oder Verteidigungs- (Blue-Teaming-)Mechanismen, um die Bewertung der Sicherheitsbereitschaft gegen reale Cyberangriffe innerhalb der CR zu unterstützen [3]. Eine CR-TB-Umgebung zur Evaluierung von Security Orchestration, Automation, and Response (SOAR)-Tools setzt auf Nessus für das Vulnerability Scanning des gesamten Netzwerks, wobei periodische Scans (mit zugehörigen, in festen Intervallen erfassten Logs) genutzt werden, um die Sicherheitslage der Umgebung zu charakterisieren und Input für die Analyse des SOAR-Verhaltens bereitzustellen [27]. In einem experimentellen Aufbau, der die Sicherheit webbasierter Kommunikation in Solar-DG-Systemen untersucht, wird Nikto neben weiteren Websicherheitstools eingesetzt, um die Sicherheit der Web-Schnittstellen zu bewerten, als ein Schritt einer breiter angelegten Evaluierung von Sicherheitskontrollen, die die allgemeine Cybersicherheitslage des Systems verbessern sollen [116].

Network Analysis & Reconnaissance

Eine Remote-Cybersicherheits-Trainingsplattform, die um Schaltschränke mit Automatisierungs- und Steuerungsgeräten herum aufgebaut ist, nutzt Nmap für Systemerkennungsaufgaben, sodass Studierende praktische Erfahrung im Erkennen und Identifizieren von Systemen in der Trainingsumgebung sammeln, während Wireshark in praxisnahen Übungen eingesetzt wird, um Netzwerkverkehr des im Betrieb befindlichen Steuerungssystems im selben Remote-Trainingsaufbau zu erfassen und zu analysieren [49]. In einem Reservoir-TB, das für Cybersicherheitsübungen eingesetzt wird, wird Wireshark vom Angreifer genutzt, um das verwendete Netzwerksegment

zu bestimmen, was Einblick in die Netzwerkkonfiguration der Zielumgebung als vorbereitenden Schritt für nachfolgende Aktionen gegen Geräte wie PLCs und HMIs im TB bietet [177].

Firewalls & Network Security Gateways

Iptables/nftables werden in einem ICS-TB als Firewall-Regeln auf Basis eines Ubuntu-22.04-Betriebssystems eingesetzt, wo sie OT-Netzwerkverkehr regulieren und auf Basis verwandter Arbeiten konfiguriert werden, um die Evaluierung einer dynamischen und zuverlässigen Intrusion-Detection-Methode gegen motivierte Angreifende innerhalb der emulierten SCADA-Umgebung zu unterstützen [45]. In einem Framework zur Sicherheitsbewertung von RAN- und Mobilgeräteumgebungen, die mit nicht- und near-real-time Radio Intelligent Controllers (RIC) verbunden sind, wird IPsec/IKEv2 auf Betriebssystemebene konfiguriert, um zwei IPsec-Tunnel aufzubauen und so die Vertraulichkeit und Integrität der Kommunikation zwischen der evaluierten Umgebung, dem RIC und der O-CU sicherzustellen [86].

Training and Practice Systems

Ein Training-and-Practice-Aufbau basiert auf einer Cyber-Range-Plattform, die quelloffene Tools nutzt, um eine isolierte Netzwerkinfrastruktur mit VPN-Zugang und unterstützenden Tools zu schaffen. In dieser Umgebung ist WordPress als Teil eines forensischen Analyse- und Übungssettings enthalten. Trainierende können eine Ziel-IP fluten, Alarmaufzeichnungen auslösen und Log-Dateien generieren, sodass sie incidentfokussierte Übungen in einem dedizierten Trainingsnetzwerk durchlaufen können [193]. Ein zweites Beispiel nutzt die EVE-NG-Plattform als Grundlage für eine Cyber-Range-Umgebung, in der die Web Application Firewall von Fortinet, Fortinets Logging-Komponenten und die Firewall von Huawei als Testgeräte innerhalb eines simulierten Netzwerks bereitgestellt werden. Der Gesamtaufbau stellt eine Infrastrukturumgebung für Netzwerkangriffs- und Verteidigungsübungen bereit, die es Lernenden ermöglicht, die Konfiguration und Bewertung dieser Sicherheitskontrollen in realistischen Trainingsszenarien zu üben [139].

Malware Analysis

Eine CR-TB-Umgebung zum Testen von SOAR-Tools integriert ThreatGrid in der Cloud neben einer Jira-Instanz für Ticketing und einem dedizierten E-Mail-System, wobei ThreatGrid für Malware-Sandbox-Tests im Rahmen der Analyse von über diesen Aufbau zugestellten Artefakten eingesetzt wird [27]. Innerhalb eines Sicherheits-TB für Systeme der nächsten Generation wird URLhaus in einem einfachen Malware-Analyse-Fall eingesetzt, um zu validieren, dass gesammelte URLs bösartig sind und zur Malware-Verbreitung genutzt werden. Dies ermöglicht es dem TB, zu messen oder zu vergleichen, wie gut ein gegebener Abwehrmechanismus gegen solche bösartigen URLs performt [113].

Reverse Engineering & Binary Analysis

In der angewandten Cybersicherheits-Ausbildungsumgebung DOJO werden Ghidra und Radare2 als Reverse-Engineering- und Binäranalyse-Tools innerhalb eines Sicherheitsübungssettings eingesetzt, wobei umfangreiches Tooling bereitgestellt wird und Studierende in einer einheitlichen Umgebung an Challenges arbeiten. Diese Tools stehen in CTF- und CTFd-basierten Aktivitäten zur Verfügung, die Linux-Nutzung, Shell-Scripting, Netzwerksicherheit, webbezogene Themen, Kernel-Sicherheit und Microarchitecture-Speculative-Execution-Angriffe innerhalb desselben Trainingsaufbaus abdecken [121].

Phishing Detection & Anti-Spoofing Tools

Eine Fallstudie zur Abmilderung von Injection- und Phishing-Angriffen in einer ICT-Umgebung nutzt PhishDetector und PhishTor zur Klassifizierung von Webseiten, sodass phishingbezogene Seiten identifiziert und gefiltert werden können, als Teil eines Aufbaus, der Sicherheitsangriffe im Zusammenhang mit Plugins adressiert und darauf abzielt, proaktiv eine sichere Umgebung umzusetzen [23].

Threat Intelligence

In einer ICT-Cyberabwehr-Umgebung, die CyberAlly vorstellt, einen wissensgraphgestützten AI-Assistenten für SOC-Operationen, wird MITRE ATT&CK als Informationsquelle für GPT eingesetzt und liefert strukturiertes Bedrohungswissen, das der Assistent nutzt, um Analyst*innen mit kontextsensitiven Empfehlungen auf Basis vorheriger Red-vs.-Blue-Übungen zu unterstützen [81]. Ein zweites ICT-Szenario stellt einen graphbasierten Ansatz zur Incident-Triage vor, bei dem MITRE ATT&CK in eine schweregradbasierte Triage-Methode integriert wird, die individuelle, auf Kill-Chains basierende Angriffsgraphen mit Asset-Kritikalität kombiniert, sodass MITRE-ATT&CK-Taktiken und -Techniken Teil des Schlussfolgerungsprozesses zur Priorisierung von Cybersicherheitsvorfällen werden [153].

Endpoint Detection & Response (EDR)

Eine Cyber-Range-Testumgebung zur Evaluierung von SOAR-Tools integriert Endgame als Endpoint-Detection-and-Response-Komponente innerhalb einer vollständigen SOC-Tool-Suite, neben Elasticsearch und Kibana als SIEM sowie Suricata als NIDS, was endpunktfokussiertes Monitoring und Untersuchung über mehrere repräsentative Threat-Emulation-Szenarien hinweg ermöglicht [27]. Der hybride, SDN-basierte ICS-Sicherheits-Proof-of-Concept nutzt pigrelay als Alert-Weiterleitungskomponente: Snort läuft im Netzwerk-Socket-Modus, und ein pigrelay-Skript leitet dessen Alarme an den SDN-Controller weiter, was die Erkennung und Reaktion auf Netzwerkkanal-Angriffe in den evaluierten industriellen Umgebungen unterstützt [102].

Incident Management & Response

Innerhalb der DefAtt-Plattform für virtuelle Cyber-Labs zur Ausbildung und Schulung im Bereich Netzwerksicherheit lösen in der überwachten Umgebung erkannte Anomalien Alarme aus, die an TheHive weitergeleitet werden, das für das Incident Management eingesetzt wird, indem es diese Alarme sammelt und verarbeitet, als Teil der Behandlung netzwerkbasierter Angriffe und deren Abwehr in der stark automatisierten Range [104].

Deception & Honeypot Systems

Ein ICS-TB zur Evaluierung eines dynamischen und zuverlässigen Intrusion-Detection-Ansatzes setzt Honeyd v.1.5c als Honeypot ein, der eingehenden Netzwerkverkehr auf einen weiteren ScadaBR-Server spiegelt und damit die Bewertung der vorgeschlagenen Methode gegen motivierte Angreifende innerhalb der SCADA-Umgebung unterstützt [45].

Application Security Testing

In einer ICT-virtuellen Umgebung, die Sicherheitsszenarien und deren Bereitstellung mithilfe von Ansible automatisiert, wird Contrast Security in der Subdomäne Application Security Testing als Blue-Team-Mechanismus eingesetzt und fungiert als defensive Anwendung innerhalb eines Sets von Apps, die jeweils entweder Angriffs- (Red-Teaming) oder Verteidigungs- (Blue-Teaming-)Fähigkeiten bereitstellen, um die Sicherheitsbereitschaft gegen reale Cyberangriffe innerhalb der Range-Umgebung zu bewerten [3].

Security Hardening

In einem Framework zur Sicherheitsbewertung von O-RAN-Mobilfunknetzausrüstung, die mit nicht- und near-real-time RICs verbunden ist, wird eine virtuelle Maschine mit Ubuntu durch Anwendung eines Hardening-Verfahrens auf Basis des Ubuntu Security Guide für Center for Internet Security (CIS)-konformes Ubuntu Long-Term Support (LTS) abgesichert, sodass der CIS Ubuntu Security Guide die konkrete Grundlage für das Hardening der evaluierten Umgebung liefert [86].

Tabelle 6: Top-10-Technologien je Subdomäne für Blue Team Operations. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.7. Portal Services

Diese *Technology Domain* umfasst Portal Services, die über CRs und TBs hinweg eingesetzt werden. Abbildung 14 quantifiziert die Abdeckung nach Domäne und Subdomäne. ICT weist mit 19 Nennungen die höchste Gesamtaktivität auf, gefolgt von RAN & Mobile Devices (6), ICS (5), Power Systems (3) und IoT/IIoT (1). Über die Subdomänen hinweg dominiert User Access mit 25 Nennungen. Admin Access (4) und Authentication (2) sind seltener. Identity & Access Management (Identity and Access Management (IAM)) (2) und Authorization (1) sind selten. Auf Ebene der Domäne-Subdomäne-Details konzentriert sich User Access auf ICT (13), mit weiterer Nutzung in RAN & Mobile Devices (5), ICS (4), Power Systems (2) und IoT/IIoT (1). Admin Access tritt in ICT (3) und Power Systems (1) auf. Authentication wird nur in ICT (2) berichtet. IAM wird in ICS (1) und RAN & Mobile Devices (1) verzeichnet. Authorization tritt einmal in ICT (1) auf. Insgesamt konzentrieren sich Portal Services im Datensatz primär auf User Access, während administrative, authentifizierungs- und identitätsbezogene Kontrollen selektiv dokumentiert werden und weitgehend auf ICT konzentriert sind, wobei ICS isolierte IAM-Nutzung beisteuert und RAN & Mobile Devices gezielte Access-Management-Einträge ergänzt.

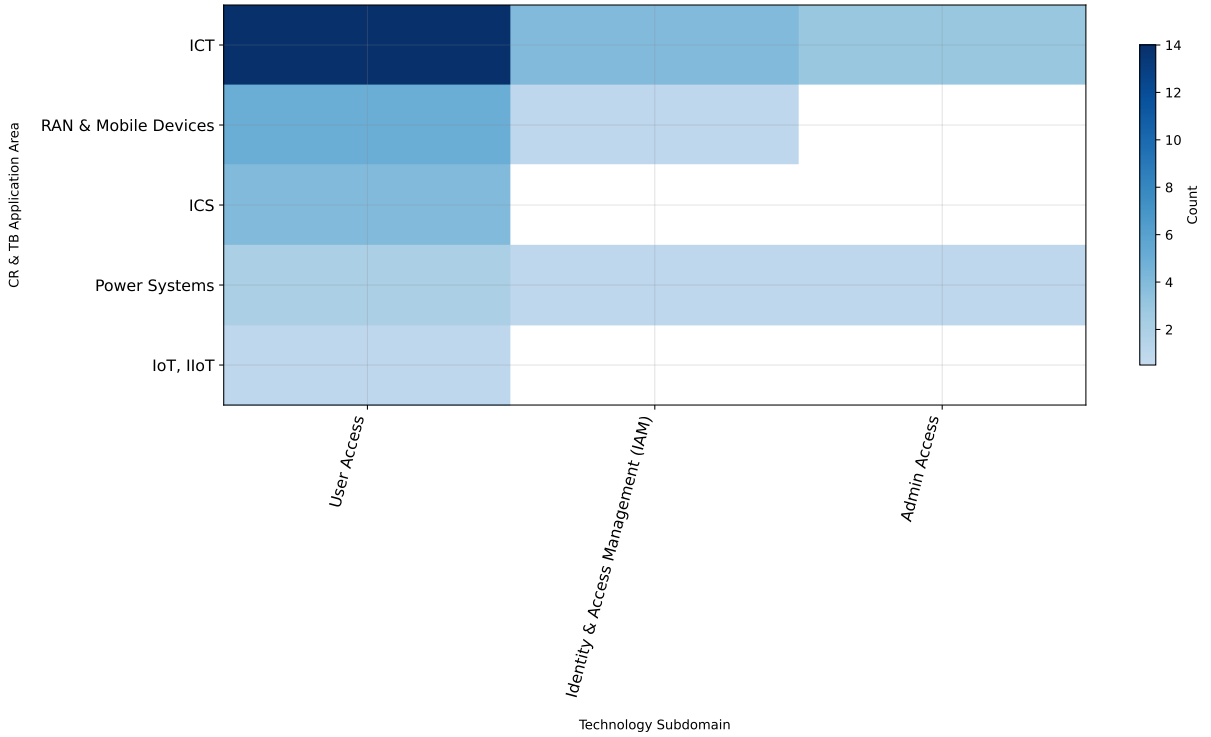


Abbildung 14: Verteilung der Portal-Services-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

User Access

In einer Industrie-4.0-fokussierten Cyber-Range-Plattform wird OpenSSH eingesetzt, um Shell-Zugriff und Dateiübertragungen (über Secure Copy Protocol (SCP)) auf die containerisierte Trainingsumgebung bereitzustellen, was es Administrator*innen und Lehrenden ermöglicht, Docker-Container auf dem Server zu konfigurieren und die quelloffenen Dienste zu verwalten, die der Cyber Range zugrunde liegen [193]. Innerhalb der angewandten Cybersicherheits-Ausbildungsumgebung DOJO stützt OpenSSH den Zugriff der Studierenden auf ihre Umgebung, indem Lernende einen öffentlichen Schlüssel hochladen und sich anschließend bei ihren indivi-

duellen Linux-basierten Trainingsinstanzen anmelden können, was CTF-artige Übungen und praxisnahes Üben in Shell-Scripting, Netzwerktechnik und verwandten Themen unterstützt [121]. In der Cyber-Arena-Plattform für skalierbare Cybersicherheitsausbildung stellt Apache Guacamole browserbasierten Fernzugriff für Studierende bereit, wobei ein Guacamole-Server über eine öffentliche IP exponiert wird, sodass Lernende von jedem Internetstandort aus über eine Web-Oberfläche auf ihre Lab-Umgebungen zugreifen können, ohne zusätzliche Client-Software installieren zu müssen [68]. In einer IoT/IIoT-Sicherheitstrainingsumgebung für Systementwickler*innen wird Apache Guacamole für das Verwalten des Zugriffs auf Linux-Container eingesetzt, wobei der Nutzerzugriff auf containerisierte Trainingsinstanzen über das Guacamole-Gateway abgewickelt wird, als Teil einer Methodik, die IoT-Sicherheitsthemen in projektbasiertes Lernen integriert [18].

Admin Access

In einer Krisenmanagement-Übungsumgebung, in der Organisationen simulierten Cyberangriffen ausgesetzt werden, wird OpenSSH auf allen Rechnern installiert und aktiviert, um Secure Shell (SSH)-Verbindungen bereitzustellen, sodass Administrator*innen im Rahmen der Schulung von Cybersicherheitsfachkräften in der Entscheidungsfindung innerhalb des Übungsaufbaus per SSH auf die Hosts remote zugreifen und diese verwalten können [150]. In einer Stromsystem-Infrastruktur für elektrische Umspannwerke, die für Tests und Evaluierung von Cyberangriffen und Incident-Response-Verfahren eingesetzt wird, bietet Apache Guacamole browserbasierten Fernzugriff auf die Enclave-Umgebung, was es Administrator*innen ermöglicht, während Cyberangriffs-Evaluierungs- und Trainingsaktivitäten über eine sichere Web-Oberfläche auf Systeme innerhalb des Umspannwerks-TB zuzugreifen [69].

Identity & Access Management (IAM)

In einer Cyber-Range-Technologieplattform, die virtuelle und praxisnahe Komponenten kombiniert, um höhere Stufen erfahrungsbasierten Lernens zu ermöglichen, wird Authentik als zentrales Identity-and-Access-Management-System für die Proxmox-basierte Infrastruktur eingesetzt, während DUO Two-Factor Authentication (2FA) Multi-Factor Authentication (MFA) durch einen plugin-gestützten Mechanismus zur Speicherung und Generierung von One-Time Passcodes (OTPs) für Nutzeranmeldungen ergänzt [66]. In einer ICT-Umgebung, die zur Evaluierung eines neuen graphbasierten Ansatzes für Incident Handling eingesetzt wird, stellt Windows Active Directory Authentifizierung und Rollenverwaltung für alle Arbeitsstationen und Server in der internen Windows-Domäne bereit, wobei die Domäneninfrastruktur (einschließlich der Active-Directory- und DNS-Server) den Host-Kontext liefert, dessen Alarme später von der vorgeschlagenen Triage-Methode analysiert werden [153]. Eine Stromsystem-Sicherheitsstudie nutzt Windows Active Directory innerhalb der CENTER-Energy-TB-Architektur, wobei OSSEC-Agenten auf Rechnern auf mehreren Ebenen laufen und einige Feldgerätecontroller Windows-basierte Betriebssysteme nutzen, sodass domänenbasierte Authentifizierung und Rollenverwaltung die Defense-in-Depth-Struktur der evaluierten Stromsystem-Testumgebung unterstützen [128].

Tabelle 7: Top-10-Technologien je Subdomäne für Portal Services. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.8. Management

Diese *Technology Domain* umfasst Management-Funktionen, die über CRs und TBs hinweg eingesetzt werden. Abbildung 15 quantifiziert die Abdeckung nach *Anwendungsbereich* und Subdomäne. ICT führt insgesamt mit 18 Nennungen, gefolgt von ICS (7). IoT/IIoT und Power Systems machen jeweils 2 Nennungen aus, und Intelligent Transportation Systems macht 1 Nennung aus. Über die Subdomänen hinweg ist Platform & Environment Management am häufigsten (7), gefolgt von Identity & Access Management (IAM) (5). Asset & Infrastructure Management und Learning Management System summieren sich auf jeweils 4. Operations Management und User Management summieren sich auf jeweils 3. Content and Document Management und Workflow & Orchestration summieren sich auf jeweils 2. ICT weist die breiteste funktionale Streuung auf und deckt alle aufgeführten Management-Subdomänen ab, mit den höchsten Werten bei Learning Management System (4), Operations Management (3) und User Management (3). ICS konzentriert sich stark auf Platform & Environment Management (5) und trägt Identity & Access Management (2) bei. Power Systems berichtet nur Asset & Infrastructure Management (2). IoT/IIoT berichtet Platform & Environment Management (1) und Workflow & Orchestration (1). Intelligent Transportation Systems berichtet einen einzelnen Eintrag bei Identity & Access Management (1). Insgesamt sind Management-Fähigkeiten in ICT verankert, während andere *Anwendungsbereiche* eine schmale Abdeckung zeigen, die hauptsächlich Plattformadministration in ICS und Asset Management in Power Systems umfasst.

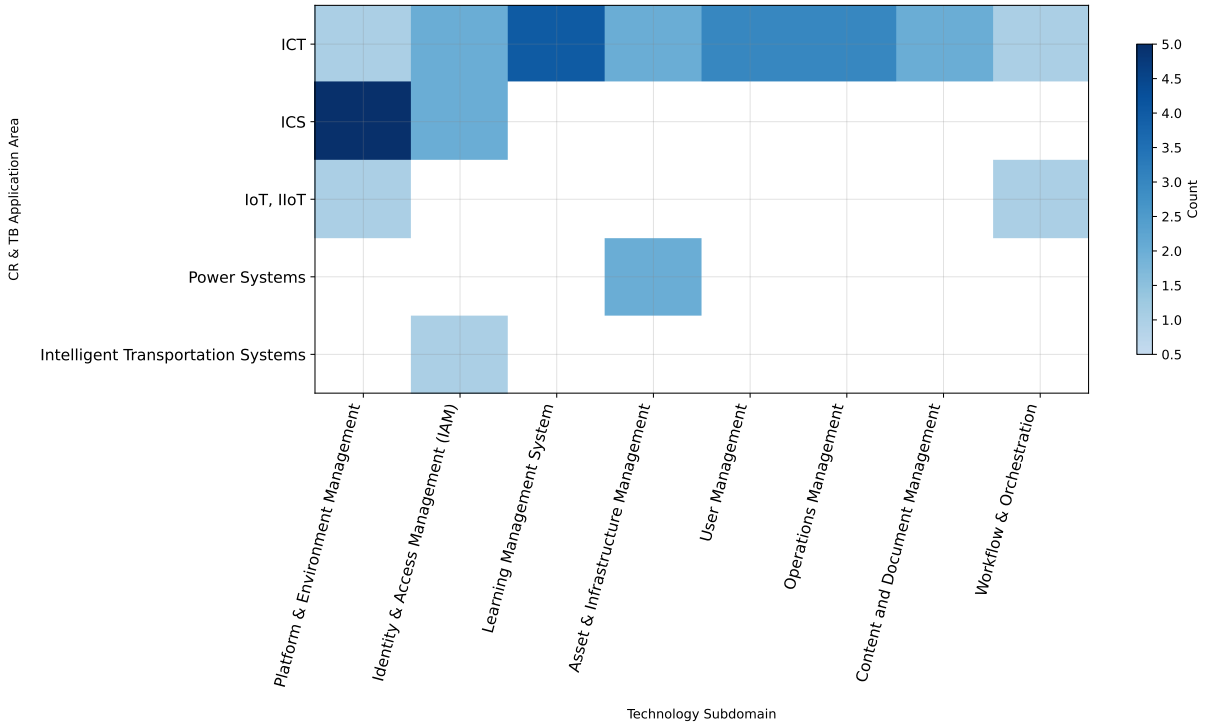


Abbildung 15: Verteilung der Management-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Platform & Environment Management
Die angewandte Cybersicherheits-Ausbildungsplattform DOJO nutzt 9p für transparentes Dateisystem-Mapping zwischen QEMU-VMs und Containern, sodass die Umgebung der Lernenden nahtlos über VMs- und Container-Grenzen hinweg auf Dateien zugreifen kann, in browserbasierten CTF-artigen Labs zu Themen von Linux-Nutzung bis Microarchitecture-Angriffen [121]. In der webbasierten Cyber Range CyberIoT für IoT hostet ein Linux, Apache, MySQL, and PHP (LAMP)-Stack die dreischichtige Webanwendung, wobei LAMP die Web- und Datenbankschichten bereitstellt, die die Instanziierung, Ausführung und den Betrieb IoT-fokussierter Cybersicherheitstrainingsübungen unterstützen [163].

Identity & Directory Access Management (IAM)
Windows Active Directory wird in einer groß angelegten ICT-Cyber-Range-Architektur eingesetzt, um virtualisierte Verzeichnis- und Authentifizierungsdienste bereitzustellen, wobei Active-Directory-, DNS- und Domänencontroller-Rollen bereitgestellt werden, um Nutzende und Systeme konsistent über die Range-Umgebung hinweg zu verwalten [127]. Das Security Credential Management System (SCMS) erscheint in einer Co-Simulationsplattform für intelligente Verkehrssysteme im Bereich vernetztes und automatisiertes Fahren, wo es sichere und datenschutzbewusste Kommunikation zwischen Geräten ermöglicht, indem es zertifikatsbasierte Zugangsdaten für den Informationsaustausch in der Testumgebung verwaltet [1].

Learning Management System
Die akademische Cyber Range Tectonic nutzt Moodle zur Bereitstellung und Erfassung von Bewertungen, wobei Studierende Flags einreichen und Fragebögen über die Moodle-Plattform ausfüllen, sodass die Bewertung ihrer Leistung eng an die Trainingsszenarien der Range gekoppelt

ist [64]. In der containerbasierten Cyber Range ETHACA wird Moodle als quelloffenes Learning-Management-System eingesetzt, um Lernergebnisse und Monitoring zu verbessern, wobei das LMS neben weiteren Komponenten zur Stärkung von Cybersicherheits-Lernerfahrungen in die quelloffene Cyber-Range-Infrastruktur integriert ist [37]. Die CyberSim-Lab-Umgebung integriert die Bazaar Collaborative Learning Environment als kollaborative Lernplattform, die Cybersicherheits-Labs unterstützt, wobei Bazaar Aktivitäten zugrunde liegt, die um spezifische Lernergebnisse herum gestaltet sind und kollaboratives Lernen, technische Simulation sowie metakognitives Engagement über unterschiedliche Lerngruppen hinweg fördert [125].

Asset & Infrastructure Management

Innerhalb des sicheren TB CENTER Energy für Stromnetze wird Dragos OT Asset Visibility and Inventory eingesetzt, um Asset-Sichtbarkeit bereitzustellen und ein Inventar der OT-Komponenten zu pflegen, während Windows Active Directory Authentifizierung und Rollenverwaltung für alle windows-basierten Arbeitsstationen und Server in der Umgebung übernimmt [128]. Die auf KYPO-CRP basierende Smart-Grid-Cyber-Range nutzt GIT als Versionierungs-Backend für Szenario-, Geräte- und Netzwerkbeschreibungen und speichert diese Elemente als Textdateien, die über das GIT-Repository in der Plattform hochgeladen und gepflegt werden [94].

User Management

Die CyberExpert-Plattform zum Erwerb von Cybersicherheitsexpertise nutzt CSV als strukturiertes Datenaustauschformat für Studierendeninformationen, mit Skripten, die CSV-Dateien einlesen, um die Erstellung neuer Nutzerkonten in der gemischten virtuellen und praxisnahen Cyber-Range-Umgebung zu automatisieren [66]. In einer Umgebung zur Gestaltung von Cyber-Range-Übungen wird die Verwaltung von Nutzerdaten mit Google Firebase umgesetzt, das Teilnehmendeninformationen speichert und verwaltet, die vom Übungsportal und verwandten Komponenten im Einklang mit den interdisziplinären CRX-Gestaltungsprinzipien benötigt werden [60].

Operations Management

Eine SOAR-fokussierte Cyber-Range-TB-Umgebung konfiguriert Jira als Ticketing- und Incident-Management-System in der Cloud und nutzt Jira zur Verwaltung von Tickets, die während Security-Orchestration-Experimenten erzeugt werden, sowie zur Unterstützung des gesamten Workflows rund um das Testen von SOAR-Tools [27]. Für logbasierte Anomalieerkennung auf Cyber-Range-Plattformen wird Pm4py eingesetzt, um Process-Mining-Analysen auf erfassten Logs durchzuführen, was Process Discovery und Conformance Checking bereitstellt, die die Analyse von Angriffsszenarien wie Path Traversal mit Remote Code Execution und Privilege Escalation unterstützen [24].

Content and Document Management

Eine groß angelegte ICT-Cyber-Range-Architektur setzt SharePoint als Kollaborations- und Dokumentationsplattform zur Verteilung von Trainingsmaterialien und Übungsartefakten ein, und dieselbe Umgebung betreibt Windows Active Directory, um virtualisierte Active-Directory-, DNS- und Domänencontroller-Dienste zur Verwaltung von Nutzenden und Systemen über die Range hinweg bereitzustellen [127]. WordPress dient als Content-Management-System in einem cloudbasierten Cyber-Range-Blueprint für kostengünstige Sicherheitsforschung, wo es für die Komponente „Imitating Human Behaviour“ eingesetzt wird, die die vom Range-Design benötigten Webinhalte strukturiert und bereitstellt [196].

Workflow & Orchestration
Die CyberAlly-Umgebung integriert Cydarm als Case-Management-Backend für Workflow und Orchestrierung, wobei CyberAlly Task-Tickets in Cydarm generiert und verknüpft, sodass verdächtige Alarme effizient innerhalb des Incident-Response-Prozesses behandelt werden können [81]. Innerhalb des Cyber-TB SAir-IIoT für Smart Airports dient JSON als Datenformat für die Konfiguration und Kennzeichnung von Netzwerkverkehrsanalyse-Daten und unterstützt die Definition und Handhabung von Angriffs- und Verteidigungsszenarien in IIoT-basierten Smart-Airport-Experimenten [84].

Tabelle 8: Top-10-Technologien je Subdomäne für Management. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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

4.3.9. Network Infrastructure

Diese *Technology Domain* beschreibt Technologien, die ausschließlich in dem Core-Technology-Layer eingesetzt werden, und umfasst Network-Infrastructure-Fähigkeiten, die CRs und TBs unterstützen. Abbildung 16 quantifiziert die Abdeckung nach *Anwendungsbereich* und Subdomäne. ICT führt mit 19 Nennungen, gefolgt von ICS (13), Power Systems (11), IoT/IIoT (9), CPS (4) und RAN & Mobile Devices (1). Über die Subdomänen hinweg dominiert Network Virtualization mit 46 Nennungen, Firewall and Routing Platform macht 10 aus, und Reverse Proxy tritt einmal auf. Network Virtualization wird in allen *Anwendungsbereichen* berichtet und ist am häufigsten in ICT (14), Power Systems (10) und ICS (9), mit zusätzlichen Nennungen in IoT/IIoT (8), CPS (4) und RAN & Mobile Devices (1). Firewall and Routing Platform konzentriert sich auf ICT (4) und ICS (4), mit Einzeleinträgen in IoT/IIoT (1) und Power Systems (1). Reverse Proxy wird nur einmal in ICT beobachtet. Insgesamt zeigen die Daten, dass virtualisiertes Networking das Rückgrat der Konnektivität über die *Anwendungsbereiche* hinweg bildet, während Firewall- und Routing-Plattformen selektive Perimeterfunktionen bereitstellen und die Nutzung von Reverse Proxys selten ist.

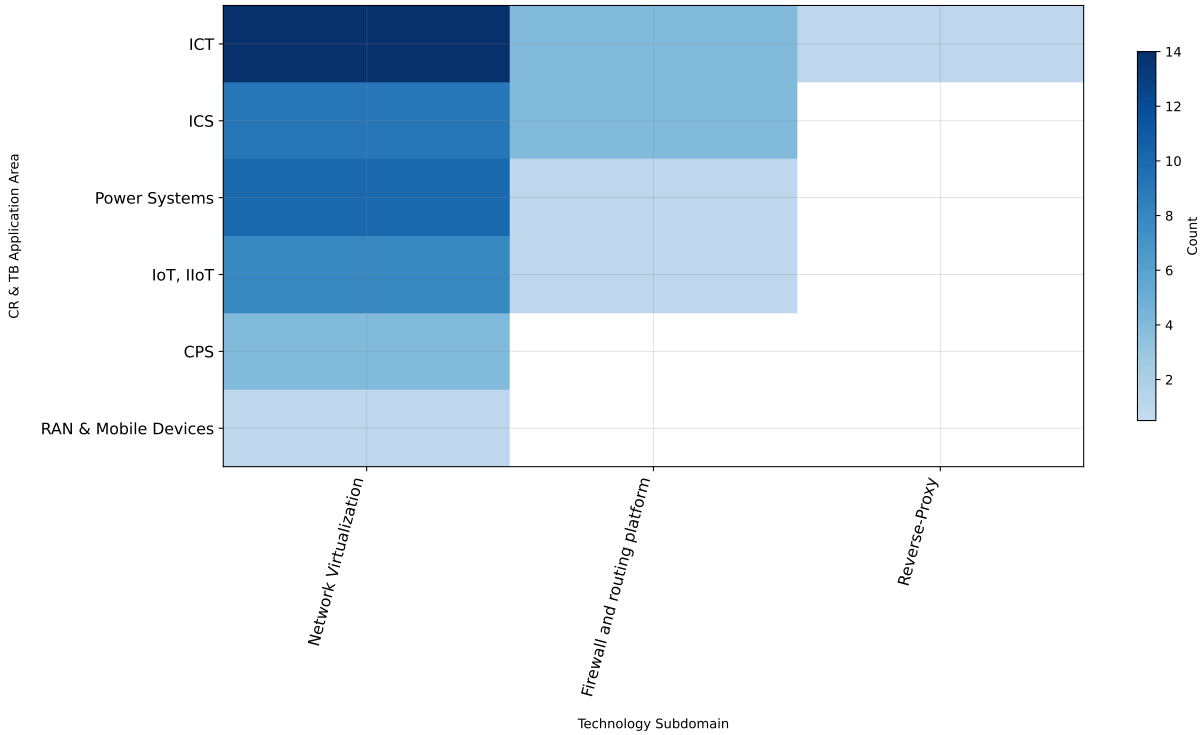


Abbildung 16: Verteilung der Network-Infrastructure-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Network Virtualization

Ein TB für autonome Operationen in OT-Anlagen platziert das gesamte OT-Netzwerk in einer einzigen Mininet-Instanz, was es ermöglicht, unterschiedliche Angriffstypen, die zu Anlageninstabilität führen, innerhalb eines kontrollierten virtuellen Netzwerks auszulösen und zu beobachten [141]. Eine ICS-fokussierte Cyber Range zur Evaluierung authentischer Trainingsübungen nutzt Mininet als Netzwerksimulationstool, um die Kommunikation industrieller Steuerungssysteme innerhalb der Range zu emulieren, sodass das Framework Übungen wie die CRX Iceberg unter realistischen virtuellen Netzwerkbedingungen instanziieren und bewerten kann [61]. Ein SDN-basierter ICS-Proof-of-Concept für Erkennung und Reaktion setzt OpenvSwitch (OvS) als OpenFlow-Switch ein, der die Netzwerksimulation zwischen Snort und dem RYU-SDN-Controller realisiert, wenn nicht zeitkritische industrielle Umgebungen bewertet werden [102]. Das automatisierte Framework DefAtt für netzwerkbasierte Angriffe und Verteidigung nutzt eine OvS-Engine, um die zugrunde liegende Infrastruktur aufzubauen, indem Bridges und Ports erstellt werden, an die virtuelle Maschinen und Docker-Container für die Sicherheitsevaluierung angebunden werden [104].

Firewall and Routing Platform

Ein vielseitiges Cybersicherheits-TB, TROY, setzt acht pfSense-2.6-Firewalls ein, um Subnetze und DMZs aufzubauen, wobei jede Firewall Traffic zwischen Segmenten filtert und weiterleitet, um den Vergleich quelloffener Cybersicherheits-Datensätze und TBs zu unterstützen [159]. Eine andere virtualisierte Umgebung platziert eine pfSense-basierte VM im Zentrum des TB, wo sie Firewall- und Routing-Funktionalität kombiniert, um Traffic zwischen dem Management-Server, den Clusterservern und dem Internet zu segmentieren, während Modbus-Protokollschwachstellen untersucht werden [197]. Ein Cyber-Defense-Übungsaufbau für Studierende setzt OPNSense ein, um Richtlinien zwischen mehreren Subnetzen durchzusetzen und Routing sowie Firewalling bereitzustellen, wobei dieselbe Instanz den Unternehmensteil der Umgebung mit einem

simulierten Internet für realistische Traffic-Bedingungen verbindet [152]. Logbasierte Anomalieerkennungsexperimente stützen sich auf eine OPNSense-VM, die auf einem Proxmox-Server läuft, als Firewalling-Komponente, die die Infrastruktur schützt, deren Logs auf Path Traversal, Remote Code Execution und Privilege-Escalation-Szenarien hin analysiert werden [24].

Reverse-Proxy Die Technologieplattform CyberExpert, die virtuelle und praxisnahe Komponenten kombiniert, stellt ihren Cyber-Range-Diensten Nginx Proxy Manager voran, um eine sichere und einfach zu verwaltende Reverse-Proxy- und Load-Balancing-Schicht bereitzustellen, die höhere Stufen erfahrungsbasierten Lernens unterstützt [66].

Tabelle 9: Top-10-Technologien je Subdomäne für Network Infrastructure. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	Nennungen	Versch. Tech.	Top-10-Technologien	Domänen
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 modeling* (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

4.3.10. Scenario

Diese Domäne beschreibt die Technologien, die zur Umsetzung eines breiten Spektrums an Szenarien in CRs und TBs eingesetzt werden. Abbildung 17 quantifiziert die Abdeckung nach *Anwendungsbereich* und Szenario-Subdomäne. Die Gesamtaktivität ist am höchsten in ICT und Power Systems mit jeweils 107 Nennungen, gefolgt von ICS (106), CPS (92), RAN & Mobile Devices (66), IoT/IIoT (51) und Intelligent Transportation Systems (39). Über die Subdomänen hinweg dominiert Infrastructure mit 316 Nennungen, gefolgt von Simulation and Emulation (125), Create/Edit (66) und Traffic Generation (46). Controlling wird 13-mal berichtet. User Activity Simulation und User Behavior Simulation treten jeweils nur einmal auf, und zwar nur in ICT. Auf Ebene der *Anwendungsbereiche* betonen ICS und Power Systems primär Infrastructure (63 bzw. 61) und Simulation and Emulation (27 bzw. 26). ICT kombiniert Infrastructure (55) mit Create/Edit (27) und Traffic Generation (20), während die übrigen Subdomänen in ICT nur marginal auftreten. CPS zeigt eine nahezu ausgeglichene Verteilung zwischen Infrastructure (43) und Simulation and Emulation (39). RAN & Mobile Devices bleibt infrastrukturfokussiert (47) mit geringeren Werten in den übrigen Subdomänen. IoT/IIoT kombiniert Infrastructure (32) mit nennenswerter Traffic Generation (16). Intelligent Transportation Systems fällt auf, da Simulation and Emulation (22) Infrastructure (15) übersteigt. Insgesamt bleiben Szenarioumsetzungen über die meisten *Anwendungsbereiche* hinweg infrastrukturzentriert, wobei Simulation and Emulation die wichtigste ergänzende Aktivität darstellt. Create/Edit und Traffic Generation konzentrieren sich auf ICT und IoT/IIoT, während verhaltensorientierte Nutzersimulation in der untersuchten Literatur nahezu nicht vorkommt.

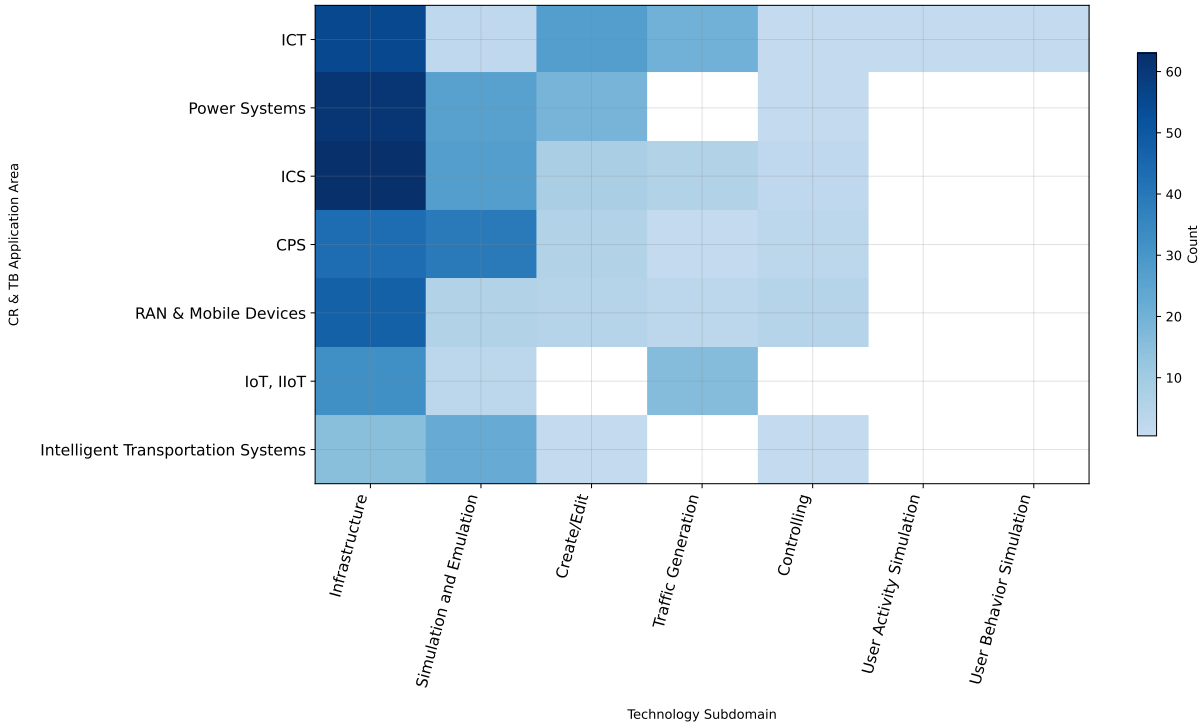


Abbildung 17: Verteilung der Scenario-Subdomänen über die Anwendungsbereiche von Cyber Ranges.

Infrastructure

Ein Smart-Grid-TB nutzt zwei Ubuntu-VMs mit rapid-SCADA und pySCADA, um Stromsystemstatistiken über das Modbus-TCP-Protokoll von PLCs abzurufen, diese Daten in einer SQL-Datenbank zu speichern und über eine Engineering-Workstation bereitzustellen, während eine separate VM als zentraler Log-Server fungiert, um ein erklärbares, selbstbewusstes Intrusion-Detection- und Active-Response-Framework für das Netz zu unterstützen [215]. In einem ICS-TB, das reale Stromsystemumgebungen mit HMIs, PLCs, Power-Quality-Monitoren und Protokollen wie Modbus, IEC 60870-5-104 und IEC 61850 nachbildet, gehört Modbus zu den zentralen Kommunikationsprotokollen, die von einer Toolchain genutzt werden, die die Generierung von Angriffsszenarien rund um ein gemeinsames Datenmodell automatisiert und damit die Integration realer Angriffsszenarien ermöglicht, die die Schritte manueller Penetrationstester*innen nachbilden [13]. Eine Studie zu Schutz-IEDs hebt IEC 61850 GOOSE als Protokoll hervor, das aufgrund niedriger Latenzanforderungen, Multicast-Paketzustellung und fehlender Verschlüsselung verwundbar ist, und nutzt dieses Protokoll als Grundlage zur Bewertung, wie unterschiedliche kommerzielle IED-Implementierungen auf Angriffe reagieren und sich davon erholen, um die Sicherheitsimplikationen GOOSE-basierter Kommunikation zu verstehen [25]. Eine Digital-Power-Twin-Umgebung für Smart Grids setzt GOOSE für zeitkritische Kommunikation zwischen IEDs im physischen TB und im Digital Twin ein, wobei GOOSE-Nachrichten Anomalie-Alarme übertragen und unmittelbare Schutzmaßnahmen auslösen. Dies ermöglicht es Nutzenden, reale Angriffe und Gegenmaßnahmen einzusetzen und deren Wirksamkeit in einer leichter modifizierbaren und reproduzierbaren Umgebung als einem rein physischen Aufbau zu untersuchen [74].

Simulation and Emulation

Eine Co-Simulationsplattform für Stromverteilungssysteme modelliert die Cyber-Schicht in MATLAB/Simulink, während das Stromsystem in DIgSILENT PowerFactory abgebildet wird, mit Echtzeit-Datenaustausch über einen Matrikon-Open Platform Communications (OPC)-Server und

Distributed Network Protocol 3 (DNP3)-Kommunikation, die in dedizierter Software modelliert wird. Dies ermöglicht den Einsatz modellbasierten Reinforcement Learnings zur Erkennung koordinierter cyber-physischer Angriffsereignisse und zur Ableitung der Ziele der Angreifenden [154]. Eine weitere Studie zu oszillierenden Lastangriffen, die von kompromittierten EV-Ladestationen ausgehen, baut das IEEE-New-England-39-Bus-System in MATLAB/Simulink auf und nutzt dieses Systemstabilitätsmodell, um gutartige und bösartige Datensätze zu synthetisieren, die einem edgebasierten Erkennungs- und Lokalisierungsansatz zugrunde liegen, der Cyber- und physische Merkmale mit Deep-Learning-Methoden kombiniert [156]. In einem Echtzeit-Co-Simulations-TB für das öffentliche EV-Lade-Ökosystem läuft der Opal-RT-HYPERSIM-Simulator auf einer Windows-VM, die mit OP5650-Echtzeit-Digitalsimulator-Hardware verbunden ist, um das mit EV-Infrastruktur verknüpfte Stromnetz abzubilden. Dies stellt Echtzeitsimulationen bereit, die eine Monitoring-Plattform zur Erkennung EV-basierter Cyberangriffe speisen [147]. Ein TB für großflächige Stromsystemanwendungen setzt einen OPAL-RT-Echtzeit-Digitalsimulator ein, um großmaßstäbliche Netzmodelle zu hosten, und nutzt die IEC 61850-I/O-Schnittstelle von RT-LAB, um physische IEDs auf den Simulator abzubilden. Dies unterstützt eine effiziente Modellierung logischer Knoten in physischen Relais und ermöglicht Hardware-in-the-Loop-Experimente mit Geräten in Industriequalität [144].

Create/Edit

In einem TB für cyber-physische Sicherheit von Stromverteilnetzen wird Modbus als weit verbreitetes Client-Server-Protokoll in der industriellen Automatisierung charakterisiert, wobei SCADA-Systeme in Leitstellen als Modbus-Clients fungieren, die Informationen von Remote Terminal Units als Server anfordern, und die resultierende Kommunikation genutzt wird, um die Auswirkungen von Cyberangriffen auf Verteilnetzsysteme zu analysieren [171]. Ein weiteres TB zur Evaluierung angriffsresilienter Netzwerkagenten erweitert die PLC-Kapazität durch Anbindung von Modbus-TCP-Geräten, sodass zusätzliche Slave-PLCs über ein standardisiertes Adressierungssystem von den Registern einer Master-PLC lesen und in diese schreiben können, was realistische Steuerungsverkehrsmuster für Experimente erzeugt, die Angriffe auslösen, die zu OT-Anlageninstabilität führen [141]. Die Cyber Range Tectonic beschreibt jedes Szenario mithilfe einer auf YAML basierenden Spezifikationssprache, wobei YAML-Dateien Maschinen, Netzwerke und Konfigurationen definieren, die auf die Maschinen des Szenarios angewendet werden. Dies unterstützt anpassbare Netzwerkkonfigurationen, Echtzeit-Monitoring und automatisierte Angriffssimulationen, die theoretisches Wissen mit praktischen Fähigkeiten verbinden [64]. Innerhalb des CRACK-Frameworks beginnt das Szenariodesign bei Theaterelementen wie Netzwerken und Compute-Knoten und geht zu Szenarioaspekten wie Schwachstellen über, wobei das gesamte Szenario in 2385 Zeilen über 29 YAML-Dateien kodiert ist, sodass die YAML-basierte Scenario Description Language (SDL) eine deklarative Möglichkeit bietet, Elemente und deren Zusammenspiel für Design, Modellverifikation, Generierung und automatisiertes Testen von Cyber-Szenarien zu spezifizieren [151].

Traffic Generation

In einem SDN-basierten TB zur Abwehr von DDoS-Angriffen durch bösartige IoT-Systeme erzeugt curl-loader gültigen HTTP-Traffic, während weitere Tools vielfältige DDoS-Anfragemuster erstellen, sodass die Mischung aus legitimem und Angriffs-Traffic genutzt werden kann, um eine semi-überwachte Deep-Extreme-Learning-Machine sowie einen Mitigation-Algorithmus, der in den SDN-Controller eingebettet ist, zu evaluieren [142]. Ein hierarchisches DDoS-Abwehrsystem für SDN-Umgebungen nutzt ebenfalls curl-loader, um Flash-Traffic-Lasten durch die Simulation groß angelegter HTTP-Client-Anfragen zu erstellen, und trägt so zum SDN-DAD-Datensatz bei, der legitimen Traffic, Flash-Traffic und verschiedene DDoS-Angriffe kombiniert, um Erkennungsmerkmale zu evaluieren, die die Rechenlast des Controllers minimieren [77]. In einem ICS-TB, das

ein dynamisches und zuverlässiges Intrusion-Detection-Modell evaluiert, wird Acunetix eingesetzt, um Netzwerkverkehr im gesamten TB zu generieren, wodurch die Web-Traffic-Muster erzeugt werden, gegen die die zweistufige Klassifikation und die auf Rejection basierende Zuverlässigkeitsbewertung von Netzwerkangriffen durchgeführt werden, während sich das Modell an sich entwickelnden Traffic anpasst [45].

Controlling

Ein CPS-TB auf der National Science Foundation (NSF)-AERPAW-Plattform integriert das Flower Framework, um ein Federated-Learning-Szenario zu hosten, in dem ein YOLOv8-Modell zur Objekterkennung auf Edge-Geräten wie Drohnen eingesetzt wird, und das Framework wird genutzt, um Optimierungs- und Abwehrmechanismen wie Differential Privacy und Adversarial Training für die Netzwerk-Incident-Anomalieerkennung unter gutartigen und unterschiedlich vergifteten Bedingungen zu untersuchen [85]. In einem resilienzfokussierten TB, das einen Lkw mit einem autonomen Cyberabwehrsystem und physischen Resilienzfunktionen modelliert, automatisiert OpenTAP die Ausführung von Experimenten und bietet eine GUI zur Konfiguration von Experimentschritten, was wiederholbare und systematische Durchläufe ermöglicht, die resilienzrelevante Daten erfassen, während das System Malware-Angriffen ausgesetzt wird [203].

User Activity Simulation Ein Aufbau zur Generierung von Netzwerkverkehr für CRs nutzt Selenium zusammen mit Python-Skripten, um Webseiten über Firefox zu manipulieren, wobei die Instanzen mit dem erforderlichen Browser-Add-on ausgestattet sind, sodass skriptgesteuerte Aktionen einfach über Selenium-Befehle ausgelöst werden können und zu realistischem Traffic beitragen, der die Qualität des Trainings verbessert [50].

User Behavior Simulation In einem logdaten-orientierten TB für Cybersicherheitsexperimente steuert Selenium remote ein Firefox-Browserfenster, das zu Beginn jeder Sitzung geöffnet und anschließend geschlossen wird, wodurch realistische und reproduzierbare Nutzerinteraktionsmuster erzeugt werden, die Log-Datensätze für die Intrusion-Detection-Forschung mit transparenten, anpassbaren und öffentlich verfügbaren Traces befüllen [189].

Tabelle 10: Top-10-Technologien je Subdomäne für Scenario. Hochgestellte Zeichen: * = Core Technology, † = Target Infrastructure, ‡ = Orchestration.

Technologie-Subdomäne	**Nennungen**	**Versch. Tech.**	**Top-10-Technologien**	**Domänen**
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 Behavior Simulation	1	1	Selenium (1)	ICT

5. Diskussion

Dieses Kapitel reflektiert zunächst kritisch die bei dieser Studie aufgetretenen Herausforderungen hinsichtlich Kategorisierung und Terminologie. Anschließend werden charakteristische Muster, Auffälligkeiten und Trends in der erhobenen Datengrundlage analysiert, gefolgt von einem Vergleich der technologischen Entwicklung von CRs und TBs mit den Erkenntnissen früherer Übersichtsarbeiten. Abschließend werden die Forschungsfragen aus Kapitel 1 beantwortet.

5.1. Die Herausforderungen von Kategorisierung und Terminologie

Verwandte Übersichtsarbeiten heben anhaltende Probleme in der Literatur hinsichtlich Taxonomien und Konzeptualisierungen von CRs und TBs hervor. So unterscheiden sich beispielsweise Terminologie und Taxonomien zwischen den Publikationen, und bestehende Taxonomien werden nicht einheitlich verwendet. Allerdings unterscheiden sich auch die in den Übersichtsarbeiten selbst verwendeten Architekturen und Terminologien erheblich. Tabelle 11 stellt die in diesen Übersichtsarbeiten verwendeten Architekturen und Schlüsselbegriffe gegenüber. Eine tabellarische Darstellung erfasst zwar nicht die gesamte Komplexität der Architekturen, ist jedoch ausreichend, um die wesentlichen Unterschiede hervorzuheben. Die erste Spalte listet die Vergleichskategorie auf, während die folgenden drei Spalten die entsprechenden Kategorien und deren Unterkategorien in Klammern beschreiben.

Alle Architekturen enthalten einen Einstiegspunkt oder Mechanismus für den Nutzerzugriff, verwenden dafür jedoch unterschiedliche Bezeichnungen und Detailgrade. Laut [71] umfassen Administration und Orchestrierung von Übungen sowohl Nutzer- und Asset-Management als auch Scheduling. In der Publikation von [190] wird hierfür keine eigene Schicht oder Zone definiert. Stattdessen werden verwandte Funktionen innerhalb der Cyber Range Capabilities beschrieben, etwa Reporting, Trainingsmethoden und Datenerfassung. In der von [209] vorgeschlagenen Architektur werden diese Aspekte durch die Kategorie *Management* abgedeckt. Darüber hinaus beschreibt [209] ein Testmodul, das in den beiden anderen Architekturen nicht enthalten ist. Für Orchestrierung und Provisioning (z. B. Infrastructure as Code (IaC) und APIs) sowie für die Virtualisierungs- oder Infrastrukturschicht definieren [190] und [71] jeweils eigene Kategorien, während [209] diese Aspekte kombiniert und Orchestrierung nicht explizit erwähnt. Eine Daten- oder Speicherschicht wird nur von [71] als Funktion oder Fähigkeit innerhalb der Underlying Infrastructure beschrieben. Eine eigene *Data-Storage*-Kategorie wird nur von [209] bereitgestellt, während [190] diesen Aspekt nicht explizit erwähnt. Die übrigen Vergleichskategorien treten in allen Architekturen auf, unterscheiden sich jedoch in Inhalt, Terminologie und ihrer Einordnung innerhalb der Gesamtarchitektur. Darüber hinaus wenden die zum Aufbau der Datengrundlage dieser Arbeit analysierten Publikationen diese Begriffe und Referenzarchitekturen nicht einheitlich an. Chouliaras et al. [37] gruppieren beispielsweise virtuelle Maschinen und Cloud-Dienste in eine „Environment“-Komponente, ordnen Infrastruktur-Containerisierungs- und Orchestrierungstechnologien wie Docker, YAML oder Ansible dem Bereich „Scenario“ zu und weisen Entwicklungstools wie VSCode der Orchestrierung zu. Ein weiteres Beispiel ist [64], welche Orchestrierungstools und eine IaC-Schicht trennt und eine Präsentationsschicht beschreibt, die heterogene Tools wie Moodle, Kibana und MITRE Caldera umfasst. Die Unterschiede in Architekturen und Terminologie, fehlende Kategorien für Cyber-Range-Funktionen in bestehenden Architekturen sowie die uneinheitliche Verwendung von Begriffen und architektonischen Darstellungen über die analysierten Publikationen hinweg stellten eine erhebliche Herausforderung für eine umfassende und objektive Gruppierung und Kategorisierung aller Funktionen und Technologien dar. Der gewählte Ansatz bestand darin, relevante Begriffe aus den analysierten Publikationen zu erfassen und diese zu Kategorien zu gruppieren, deren Bezeichnungen die gemeinsame semantische Bedeutung der zugeordneten Begriffe widerspiegeln. Dieser Ansatz beinhaltet

Tabelle 11: Crosswalk-Vergleich logischer Cyber-Range-Architekturen (vereinfacht).

Vergleichskategorie	**Kampourakis et al. (2025) [71]**	**Ukwandu et al. (2020) [190]**	**Yamin et al. (2020)** [209]
Nutzerzugriff / Einstiegspunkt	Control Access Zone (Authentifizierung, Autorisierung)	Users; Front-End Technologies (Webbrowser, Webserver-Technologien)	Portal (Nutzende, Admin, Client)
Administration / Orchestrierung von Übungen	Management Zone (Scheduling, Nutzer-/Asset-Management, Datenanalyse)	Cyber Range Capabilities (Szenarien, Reporting, Trainingsmethoden, Datenerfassungsmechanismus)	Management (Cyber Range, Szenario, Übung/Test)
Monitoring / Scoring / Reporting	Monitoring Zone (Monitoring, Datenerfassung/-analyse, Scoring/Reporting)	Cyber Range Capabilities (Reporting, Datenerfassungsmechanismus)	Monitoring (Erfassung, Analyse, Logging); Training & Education (Scoring, After-Action-Analyse)
Szenario-Lebenszyklus / Content-Erstellung	Learning Management and Support Zone (Szenarioentwicklung, Automatisierung, Traffic-Generierung)	Cyber Range Capabilities (Szenarien)	Scenario (Erstellen/Bearbeiten, Bereitstellen, Generieren, Ausführen, Steuern, Zerstören)
Unterstützung von Training / Pädagogik	Learning Management and Support Zone (TTPs, Traffic-Erfassung)	Cyber Range Capabilities (Trainingsmethoden, Gamification, Visualisierung)	Training and Education Module (Tutoring, Scoring, After-Action-Analyse)
Test-/Validierungsmodul	–	–	Testing Module (Testfalldefinition, Analyse & Verifikation)
Virtualisierungs-/Infrastrukturschicht	Core Infrastructure Zone: Underlying Infrastructure (Server, Netzwerkgeräte, Sicherheitsfunktionen, Software & Dienste, Speicher, Rechner & Mobilgeräte); Virtualization (AWS, OpenStack, vSphere, Docker)	Core Technologies (Emulation, Virtualisierung, Simulation, Containerisierung)	Run-time Environment (Emulieren, Simulieren, Traffic-/Angriffsgenerierung, HW, Nutzerverhaltensgenerierung)
Orchestrierung / Provisioning (IaC / APIs)	Core Infrastructure Zone: Orchestration (Kubernetes, Terraform, Ansible, API usw.)	Infrastructure Technologies: Orchestration (z. B. vSphere, Wisper usw.)	Run-time Environment (Deployment, Steuerung); (Orchestrierung nicht explizit benannt)
Daten-/Speicherschicht	Underlying Infrastructure (Storage)	–	Data Storage (Szenariodefinitionen, Regeln, Tools, Replikationsdaten, Parameter)

zwangsläufig subjektive Interpretationsentscheidungen, weshalb alternative Kategorisierungen und Zuordnungen möglich sind. Nach der Veranschaulichung der Variabilität in Terminologie und architektonischen Darstellungen, werden nun quantitative Muster im extrahierten Repository analysiert, mit Fokus auf Lücken, Auffälligkeiten und Trends über *Anwendungsbereiche*, *Zwecke*

und *Technology Domains* hinweg.

5.2. Forschungslücken, Auffälligkeiten und Trends in der Datengrundlage

Die folgenden Erkenntnisse leiten sich aus Technologien und Klassifikationen ab, die in den untersuchten Publikationen berichtet werden. Beobachtete Lücken sollten daher als „Abwesenheit im analysierten Korpus“ interpretiert werden und können auch Publikations- und Berichterstattungspraktiken widerspiegeln, anstatt das tatsächliche Fehlen solcher Technologien im realen Einsatz.

5.2.1. Anwendungsbereiche

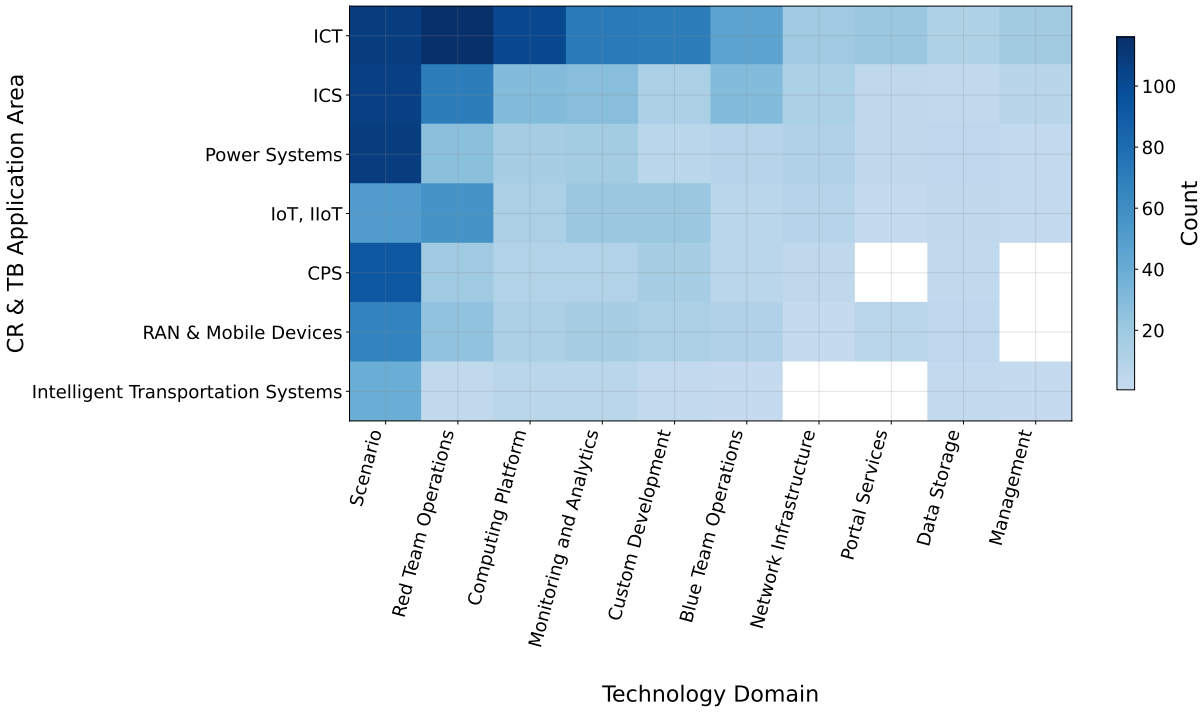


Abbildung 18: Technologieverteilung über die Anwendungsbereiche von Cyber Ranges.

Über alle *Anwendungsbereiche* hinweg (Abbildung. 18) ist die *Technology Domain Scenario* am häufigsten vertreten (578), gefolgt von *Red Team Operations* (315) und *Computing Platform* (193). Die genauen Inhalte werden in Abschnitt 4.3 beschrieben. Mehrere *Anwendungsbereiche* zeigen ein konzentrierteres Profil. In *Power Systems* sind die meisten Technologien der *Scenario*-Domäne zugeordnet (107), während andere Domänen deutlich niedrigere Werte aufweisen. ICS zeigt ebenfalls Spitzenwerte bei *Scenario* (108) und *Red Team Operations* (71), bleibt jedoch in anderen Domänen niedriger. Dies deutet darauf hin, dass sich manche *Anwendungsbereiche* auf ein engeres Set an *Technology Domains* stützen, während andere (insbesondere ICT) eine breitere Verteilung berichteter Technologien zeigen. Domänen mit geringerer Gesamtintensität, wie *Data Storage* (35), *Management* (31) und *Portal Services* (34), sind weiterhin spärlich vertreten. Zudem zeigen sich explizite Lücken, bei denen für bestimmte Kombinationen aus Anwendungsbereich und Domäne keine Technologien berichtet werden (z. B. CPS *Management*, CPS *Portal Services*, Intelligent Transportation Systems *Network Infrastructure*, Intelligent Transportation Systems *Portal Services* und RAN & Mobile Devices *Management*). Hinsichtlich der Verteilung von

CRs und TBs über die *Anwendungsbereiche* hinweg werden CRs in ICT häufiger eingesetzt als in anderen Bereichen. Ein bemerkenswertes Muster ist der häufige Einsatz von CRs in Kombination mit den *Zwecken Training and Exercises* und *Education*, insbesondere in ICT und ICS (Abbildung 4). Insgesamt deutet diese Verteilung auf eine funktionale Trennung hin: dedizierte TBs werden häufiger für *Research, Testing and Experimentation* berichtet, während CRs häufiger für *Training and Exercises* und *Education* berichtet werden. Gleichzeitig zeigen mehrere der übrigen *Anwendungsbereiche* einen Anstieg an Publikationen, insbesondere in den letzten zwei Jahren (Abbildung 3). Innerhalb von *Research, Testing and Experimentation* sind *Threat and Vulnerability Assessment*, *Attack Impact Assessment* und *Dataset Generation* die häufigsten *Use Cases*, wobei dedizierte TBs besonders häufig eingesetzt werden. Dieses Use-Case-Profil deutet darauf hin, dass experimentierorientierte Umgebungen bewertungs- und datengetriebene Aktivitäten betonen. Nur beim *Use Case Traffic Generation* werden CRs häufiger genannt als TBs (Abbildung 5), was darauf hindeutet, dass CRs bevorzugt werden könnten, wenn Traffic-Generierung in einen breiteren Szenariokontext eingebettet ist, statt als isolierte Testbed-Aufgabe behandelt zu werden. Bei den *Use Cases* von *Training and Exercises* ist der Einsatz von TBs weniger ausgeprägt, und CRs dominieren stärker. Neben allgemeinem Sicherheitstraining (das Trainingsnennungen ohne spezifischen thematischen Fokus umfasst) sind CTF, *Incident Response* und *Red vs. Blue Team*-Trainings besonders hervorstechend (Abbildung 6), was darauf hindeutet, dass interaktive und übungsorientierte *Use Cases* im untersuchten Korpus häufiger über CRs realisiert werden. Auch beim *Zweck Education* dominieren CRs. Hier werden die *Use Cases Student Assessment & Scoring*, *Learning Management Systems* und *Instructional Design* am häufigsten genannt (Abbildung 7), was auf einen starken Schwerpunkt bei strukturierter Kursintegration und Bewertungsmechanismen hindeutet.

5.2.2. Technologien

In der *Technology Domain Red Team Operations*, Subdomäne *Adversary Emulation*, wird nur eine geringe Anzahl an Tools eingesetzt, nämlich MITRE Caldera und Infection Monkey. Weitere Tools werden in den Publikationen, die Adversary Emulation durchführen, nicht berichtet, oder die Aktivitäten werden manuell umgesetzt (Abschnitt 4.3.1). Dieses begrenzte Set deutet auf eine geringe Vielfalt berichteten Toolings für Adversary Emulation in CR/TB-Implementierungen hin und könnte darauf hindeuten, dass Adversary Emulation entweder seltener als explizite Fähigkeit implementiert wird oder ohne dedizierte Tools umgesetzt und daher weniger konsistent dokumentiert wird. Metasploit kann ebenfalls für Adversary Emulation eingesetzt werden [88], wird jedoch in den analysierten Publikationen primär als Penetrationstest-Tool oder zur Durchführung einzelner Angriffe verwendet (Abschnitt 4.3.1). Dieses Beispiel veranschaulicht, dass die Technologieklassifikation vom beschriebenen Nutzungskontext abhängt und nicht von den allgemeinen Fähigkeiten der jeweiligen Technologie. Eine ähnliche Argumentation wird in Absatz 4.3.1 angewendet, wo SQL-Datenbanken nur als Ziele für SQL-Injection-Übungen eingesetzt und daher der Kategorie *Red Team Operations*, konkret unter *Training and Practice Systems*, zugeordnet werden. In der Subdomäne *Containerization* wird nahezu ausschließlich Docker eingesetzt. Nur Podman wird einmal als Alternative genannt, was darauf hindeutet, dass Docker als De-facto-Standard für Containerisierung in den untersuchten CR/TB-Implementierungen gilt. Die Subdomäne *Software Provisioning and Configuration* enthält über alle untersuchten Publikationen hinweg ebenfalls nur zwei Tools: Ansible und AWX, das eine webbasierte Benutzeroberfläche, eine REST-API und eine Task-Engine für Ansible bereitstellt (Tabelle 4), was darauf hindeutet, dass Provisioning- und Konfigurationsaufgaben ähnlich stark von einer kleinen Gruppe ausgereifter, weit verbreiteter Tools dominiert werden. Weitere Subdomänen, die nur eine einzige genannte Technologie enthalten, sind *Application Security Testing* (Contrast Security), *Incident Management & Response* (TheHive), *Security Hardening* (CIS Ubuntu Security Guide), *Honeypot Systems* (Honeyd) und *Reverse-Proxy* (Nginx Proxy Manager), was auf eine begrenzte berichtete

Abdeckung dieser Funktionsbereiche innerhalb des analysierten Korpus hindeutet. Die *Technology Domain Custom Development* enthält ebenfalls Technologien, die über alle Publikationen hinweg nur einmal auftreten. Da diese Domäne häufig Implementierungs-Stacks wie Bibliotheken und Frameworks widerspiegelt statt CR/TB-spezifische Bausteine, wird sie separat behandelt und an dieser Stelle nicht weiter vertieft.

5.2.3. Zeitliche Trends

Im Folgenden werden zeitliche Trends in der Cyber-Range- und Testbed-Literatur analysiert, um zu untersuchen, wie sich berichtete *Use Cases* und Technologien im Zeitverlauf entwickeln. Der Fokus liegt dabei auf quartalsweisen Entwicklungen. Verwendet werden normalisierte Anteile, um den generellen Anstieg des Publikationsvolumens in 2024–2025 auszugleichen. Die drei Small-Multiple-Abbildungen visualisieren quartalsweise Zeitreihen normalisierter Use-Case-Anteile innerhalb jedes *Zwecks* (*Research, Testing and Experimentation*, *Training and Exercises* und *Education*) und beziehen sich auf die Top-10-*Use Cases* je *Zweck* aus Abschnitt 4.2. Da manche Quartale nur eine geringe Anzahl an Publikationen enthalten, sind die normalisierten Kurven gelegentlich spitz und können 100 % erreichen. In diesen Fällen helfen die gestrichelten Zählkurven dabei, substanzielle Anstiege von geringen Stichprobengrößen sowie von Verschiebungen im gesamten Publikationsvolumen des jeweiligen Quartals innerhalb des betreffenden *Zwecks* zu unterscheiden. Bei *Research, Testing and Experimentation* (Abbildung 19) verschiebt sich das Profil von einer frühen Dominanz von *Threat and Vulnerability Assessment* und *Attack Impact Assessment* hin zu einem stärker diversifizierten Muster in 2024–2025, in dem *Dataset Generation* an Bedeutung gewinnt und *Cyber Security Resilience Assessment* zunehmend prominenter wird. Im selben Zeitraum werden zusätzliche lösungsorientierte und ML-bezogene Themen sichtbar und nehmen an Häufigkeit zu (z. B. *Mitigation Strategies* und *ML-based IDS/IPS*), während *Traffic Generation* vereinzelt bleibt.

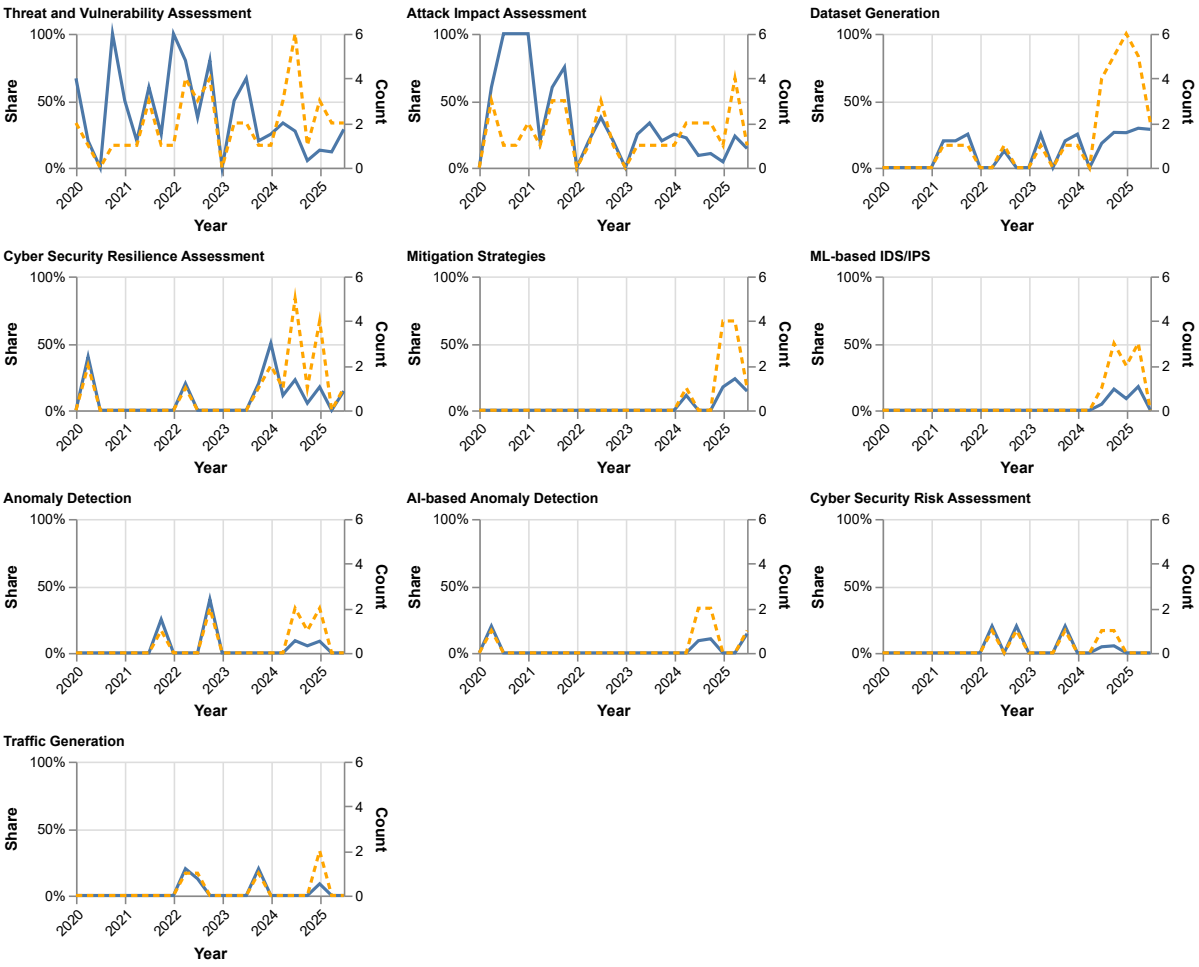


Abbildung 19: Trends im Zweck „Research, Testing, and Experimentation“.

Bei *Training and Exercises* (Abbildung 20) verschiebt sich der Schwerpunkt hin zu praxisnahen Trainingsformaten, wobei *Capture the Flag* und *General* Training im späteren Zeitraum dominieren, während frühere teambasierte und spezialisierte Formate (z. B. *Red Team vs. Blue Team*) in den jüngsten Quartalen nicht mehr berichtet werden.

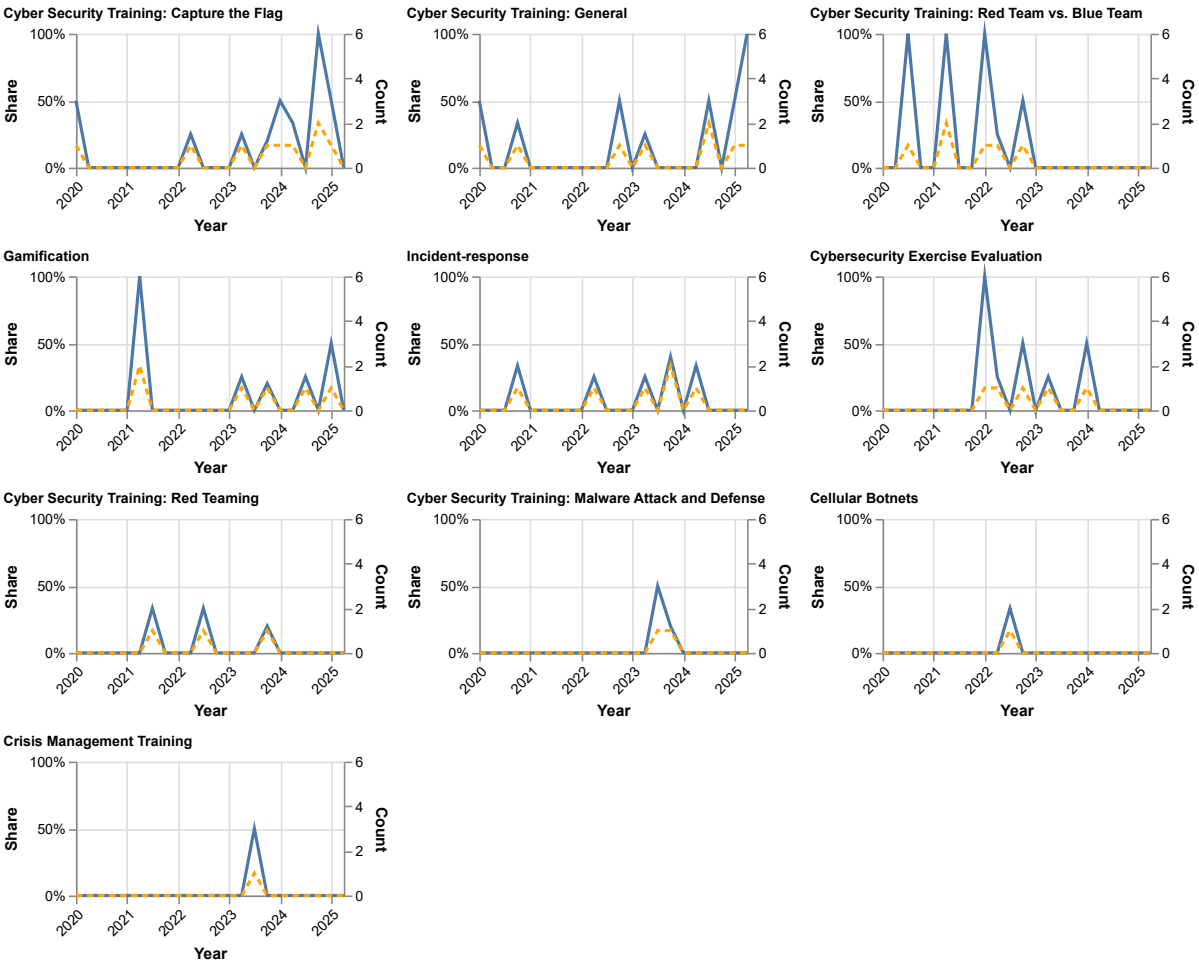


Abbildung 20: Trends im Zweck „Training and Exercises“.

Bei *Education* (Abbildung 21) bleiben *Student Assessment & Scoring* und *Learning Management Systems* die durchgängig am häufigsten berichteten Use Cases. Assessment und Scoring werden in 2024–2025 relativ prominenter. *Learning Labs* tritt nur im späteren Zeitraum auf, während *Instructional Design* vergleichsweise an Dominanz verliert.

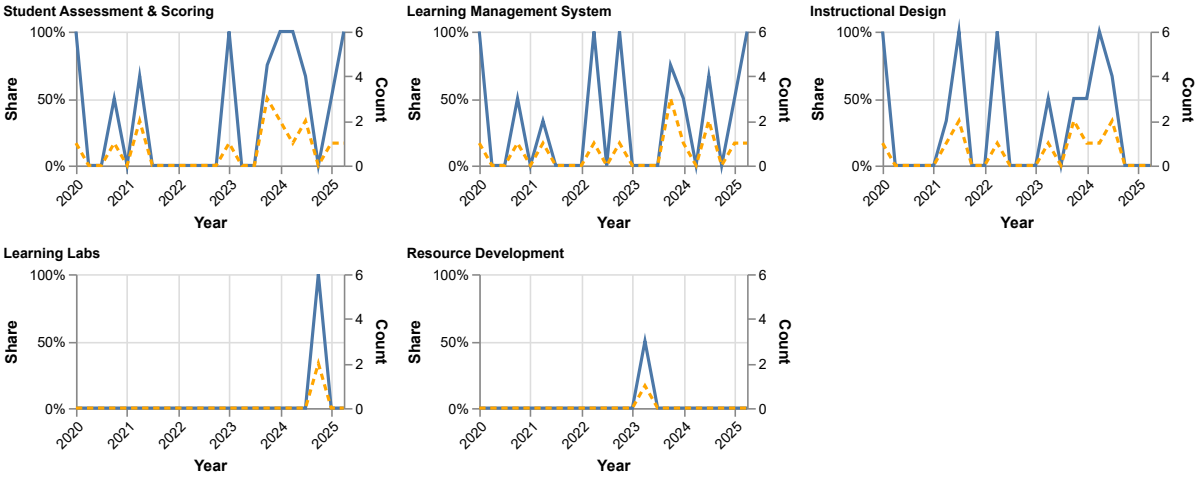


Abbildung 21: Trends im Zweck „Education“.

5.3. Technologische Entwicklung von Cyber Ranges und Testbeds

Während eine feingranulare zeitliche Trendanalyse einzelner Technologien durch uneinheitliche Berichterstattungspraktiken über die Publikationen hinweg eingeschränkt ist, liefert ein Vergleich auf Ebene der Technologiedomänen und dominanten Tools mit den Erkenntnissen früherer Übersichtsarbeiten dennoch aufschlussreiche Ergebnisse, da diese Arbeiten explizite Tool-Inventare verwenden, die einen aussagekräftigen Vergleich zwischen den Übersichtsarbeiten ermöglichen.

Hinsichtlich der Computing Platform identifizieren Yamin et al. [209] und Ukwandu et al. [190], deren Publikationskorpora sich bis 2019–2020 erstrecken, hypervisor-basierte Virtualisierung als dominant, wobei VMware am häufigsten genannt wird, während Containerisierung als leichtgewichtige und skalierbare Ergänzung zu VM-basierten Ansätzen eingeführt wird. Die vorliegende Übersichtsarbeit zeigt einen deutlichen Wandel: Docker ist die am häufigsten berichtete Containerisierungstechnologie (34 Nennungen), während traditionelle Hypervisoren weiterhin präsent, aber nicht mehr exklusiv sind, wobei VMware vSphere (9), KVM (5) und VirtualBox (11) neben containerbasierten Deployments koexistieren. Dieses Koexistenzmuster steht im Einklang mit den Erkenntnissen von Kampourakis et al. [71], die die Kombination aus Typ-2-Hypervisor, containerbasierter und privater Cloud-Virtualisierung als häufigste Konfiguration in CR-Implementierungen bis 2023 identifizieren.

Im Bereich der Orchestrierung beschreiben frühere Übersichtsarbeiten die Infrastrukturverwaltung primär in Form von Virtualisierungsschichten [190] oder Szenarioausführungsmodulen [209], ohne ein dominantes Set dedizierter Provisioning-Tools zu identifizieren. Chouliaras et al. [38] und Kampourakis et al. [71] markieren eine Entwicklung hin zu expliziten IaC-Tools, wobei die vorliegende Übersichtsarbeit Ansible (12 Nennungen) und Terraform (7 Nennungen) als führende Lösungen bestätigt und Kubernetes (4 Nennungen) Container-Orchestrierung als erkennbare architektonische Kategorie etabliert.

Im Bereich der Red Team Operations bleiben Metasploit (23 Nennungen) und Nmap (31 Nennungen) die dominanten Tools für Exploitation beziehungsweise Netzwerkscanning, was mit ihrer Prominenz in der früheren Literatur übereinstimmt [209]. Die zentrale Entwicklung ist das Aufkommen framework-basierten Toolings: MITRE ATT&CK (6 Nennungen) und MITRE Caldera (4 Nennungen) stehen für eine Verschiebung hin zu strukturierter, framework-gestützter Adversary Emulation, die in keiner der früheren Übersichtsarbeiten vorhanden ist.

Die Scenario-Domäne zeigt die stärkste Kontinuität: MATLAB/Simulink (12 Nennungen), OPAL-RT-Simulatoren (8 Nennungen) und Industrieprotokolle wie Modbus (27 Nennungen) und GOOSE (12 Nennungen) bleiben über den gesamten Zeitraum hinweg grundlegend für ICS- und Power-Systems-Szenarien, was auf stabile domänenspezifische Infrastrukturanforderungen hindeutet.

Schließlich stellen KI- und ML-Frameworks wie TensorFlow (12 Nennungen), Keras und Scikit-learn eine Technologiedomäne dar, die in den früheren Übersichtsarbeiten kein direktes Gegenstück hat. Diese Abwesenheit mag teilweise Unterschiede in Umfang und Kategorisierung zwischen den Übersichtsarbeiten widerspiegeln, steht jedoch im Einklang mit der breiteren Integration von Machine Learning in Cybersicherheits-Forschungsworkflows, die im Zeitraum 2020–2025 zu beobachten ist.

5.4. Beantwortung der Forschungsfragen

Aufbauend auf diesen Beobachtungen werden nun die in Abschnitt 1 eingeführten Forschungsfragen beantwortet.

RQ1: Welche Use Cases und *Anwendungsbereiche* für Cyber Ranges (CRs) und Testbeds (TBs) werden in der Literatur berichtet?

In der vorliegenden Literaturübersicht wurden folgende *Anwendungsbereiche* identifiziert: ICT, ICS, CPS, IoT/IIoT, RAN & Mobile Devices, Power Systems und Intelligent Transportation Systems. Abschnitt 4.2 bietet eine detailliertere Liste an *Use Cases*, gegliedert nach den CR/TB-*Zwecken Research, Testing and Experimentation*, *Training and Exercises* und *Education*. Tabelle 12 fasst die drei häufigsten *Use Cases* je *Zweck* zusammen, gereiht nach Anzahl der Artikel.

Tabelle 12: Top-3-Use-Cases je Zweck, gereiht nach Anzahl der Artikel.

Zweck	**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)

RQ2: Welche Technologien und Technologiegruppen werden zur Umsetzung spezifischer CR-/TB-Funktionen eingesetzt?

Tabelle 13 zeigt die am häufigsten berichteten Technologien für ausgewählte *Technology Subdomains* im Zusammenhang mit den in RQ1 dargestellten *Use Cases*. *Technology Subdomains* werden hier als Proxy für CR/TB-Funktionen verwendet, da die feingranularere Kategorie *Technology Functionality* primär die spezifischen Funktionalitäten einzelner Tools beschreibt. Die Kategorie *Technology Subdomain* hingegen gruppiert mehrere Tools mit ähnlichen Funktionalitäten und repräsentiert daher „Funktionen“ von CRs/TBs am besten auf einer geeigneten Abstraktionsebene. Die Tabelle zeigt eine breite Vielfalt an Technologien, darunter Tools, Protokolle, Virtualisierungstechnologien, Datenbanken und Datenformate. Sie enthält gut etablierte Technologien mit vielen Nennungen in den analysierten Publikationen, wie Metasploit (23) in der Subdomäne *Exploitation and Attack Execution*, Docker (34) in der Subdomäne *Containerisation* und Protokolle wie Modbus (28), das in Publikationen im ICS-Bereich häufig als wesentlicher Bestandteil der Szenarioinfrastruktur oder zur Angriffsausführung beschrieben wird. Gleichzeitig zeigt die Tabelle auch weniger gut abgedeckte Kategorien, wie Management oder bestimmte Datenbankkategorien, die weniger als drei unterschiedliche Tools und weniger als zehn Gesamtnennungen umfassen. Die detaillierten Ergebnisse werden in Abschnitt 5.2 bereitgestellt.

Tabelle 13: Top-3-Technologien je ausgewählter 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

RQ3: Welche Trends und bemerkenswerten Muster lassen sich in der Forschung und Entwicklung von Cyber Ranges und Testbeds beobachten (z. B. hinsichtlich Zwecke, Anwendungsbereiche und Technologien)?

In Abschnitt 5.2 werden zunächst die Spitzenwerte der *Technology Domains* über die gesamte Datengrundlage hinweg berichtet, gereiht nach Anzahl der Nennungen, nämlich *Scenario*, *Red Team Operations* und *Computing Platform*, sowie Spitzenwerte in den weniger häufig vertretenen *Anwendungsbereichen*. Zusätzlich werden Nutzungshäufigkeit von Cyber Ranges und Testbeds analysiert. Die Ergebnisse zeigen, dass Cyber Ranges am häufigsten im *Anwendungsbereich* ICT

eingesetzt werden, insbesondere in ICT für *Training, Exercises, and Education*. Darüber hinaus werden bemerkenswerte Muster in der Technologielandschaft hervorgehoben. Dies umfasst sowohl unzureichend erforschte Bereiche, wie den Einsatz von Tools für Adversary Emulation, als auch gut etablierte Technologien, die in CRs und TBs eingesetzt werden, wie Docker und Ansible.

6. Leitfaden zur Technologieauswahl für Cyber Ranges

Aufbauend auf den in den vorangehenden Kapiteln dargestellten Ergebnissen der systematischen Literaturstudie bietet dieses Kapitel eine praxisorientierte Anwendung dieser Erkenntnisse. Während die vorangehenden Kapitel den aktuellen Stand von Technologien, Use Cases und Anwendungsbereichen von CRs und TBs analytisch aufarbeiten, übersetzt dieser Leitfaden diese Ergebnisse in eine konkrete Entscheidungshilfe für die Auswahl geeigneter Technologien bei Konzeption, Beschaffung und Betrieb einer CR. Das Kapitel führt zunächst kurz in die relevanten Grundlagen ein (Zielgruppe, Bezug zur vorangehenden Literaturstudie), bevor eine Referenzarchitektur, die zugehörigen Feature-Kategorien und schließlich ein vierstufiger, praxisorientierter Auswahlprozess für konkrete Technologien vorgestellt werden.

6.1. Projektkontext

Ausgangspunkt für die Entwicklung dieses Leitfadens im Rahmen der CyberTASTE Studie, durchgeführt im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS mit Unterstützung des Bundeskanzleramts, ist die Beobachtung, dass zahlreiche sicherheitsrelevante Tätigkeiten wie Schulungen, Übungen, Tests und die Evaluierung von Sicherheitslösungen nicht auf Produktivsystemen durchgeführt werden können, da sie deren Betrieb und Verfügbarkeit gefährden würden. CRs bieten hierfür die geeignete Umgebung, stellen jedoch aufgrund der Vielzahl an verfügbaren Technologien mit unterschiedlichem Reifegrad und unterschiedlichen Lizenzmodellen eine erhebliche Auswahlherausforderung dar. Ein übergeordnetes Ziel dieser Arbeit ist es daher, alle Bedarfsgruppen bei der Auswahl der passenden Technologien zur Umsetzung spezifischer CR-Use Cases und -Features zu unterstützen. Dazu wurden in einem ersten Schritt Use Cases und Anforderungen erhoben und verfügbare Technologien systematisch analysiert, wie in den vorangehenden Kapiteln dargestellt. Das folgende Kapitel übersetzt diese Ergebnisse in eine praxisorientierte Entscheidungshilfe zur Technologieauswahl.

6.2. Zweck und Zielgruppe

Der vorliegende Leitfaden richtet sich an alle Personen und Organisationen, die eine CR konzipieren, beschaffen oder betreiben. Er adressiert gleichermaßen technische Fachkräfte wie Systems Engineers und Sicherheitsarchitekt*innen, als auch Personen mit Beschaffungs- oder Managementverantwortung, die einen fundierten Überblick über relevante Technologiebereiche und Auswahlkriterien benötigen.

Das Dokument verfolgt das Ziel, die Auswahl geeigneter Technologien für konkrete Anforderungen an eine CR zu unterstützen. Es beschreibt Technologiekategorien, ihre Funktion im Gesamtsystem sowie Kriterien, anhand derer eine informierte Entscheidung getroffen werden kann.

6.3. Grundlage: Systematische Literaturstudie

Die inhaltliche Basis dieses Leitfadens bildet die in den vorangehenden Kapiteln vorgestellte systematische Literaturstudie [107] (Abschnitte 3–5). Ergänzend dazu fließen Erkenntnisse weiterer einschlägiger Übersichtsarbeiten und Referenzarchitekturen in diesen Leitfaden ein, insbesondere hinsichtlich der Strukturierung von Features und Querschnittsbereichen, die in einzelnen Publikationen unterschiedlich verortet werden.

Für die Technologieauswahl relevant ist insbesondere der in Abschnitt 2.1 eingeführte Unterschied zwischen CR und TB: Während ein TB eine in sich geschlossene Zielinfrastruktur darstellt,

umfasst eine vollständige CR zusätzlich die Technologien zur Bereitstellung, Orchestrierung und Verwaltung dieser Infrastruktur. TBs kommen daher typischerweise mit weniger Orchestrierungswerkzeugen und einem schlankeren Core-Technology-Layer aus als vollständig ausgebaute CRs, die mehrere TB-Instanzen parallel betreiben und verwalten können.

6.4. Cyber Range Einsatzzwecke, Use Cases und Anwendungsbereiche

Die Technologieauswahl für eine CR ist unmittelbar von ihrem geplanten Einsatzzweck, den konkreten Use Cases und dem Anwendungsbereich abhängig. Diese drei Dimensionen bilden gemeinsam die Grundlage der Anforderungsanalyse und beeinflussen, welche Feature-Kategorien und Technologien für eine konkrete CR-Implementierung relevant sind. Die folgende Beschreibung stützt sich auf die in Abschnitt 4.2 eingeführte Kategorisierung.

6.4.1. Cyber Range Einsatzzwecke

In der analysierten Literatur werden drei übergeordnete Einsatzzwecke für CRs unterschieden: *Research, Testing and Experimentation*, *Training and Exercises* und *Education* (siehe Abschnitt 4.2). Diese Zwecke sind nicht immer trennscharf und können in einer CR gleichzeitig verfolgt werden.

Für die Technologieauswahl ist insbesondere relevant, dass *Research, Testing and Experimentation* überwiegend in TB-Umgebungen realisiert wird, während *Training and Exercises* und *Education* primär durch CRs umgesetzt werden (vgl. Abschnitt 5.2). Typische Use Cases je Einsatzzweck sind in Abschnitt 4.2 im Detail beschrieben.

6.4.2. Cyber Range Anwendungsbereiche

Der Anwendungsbereich beschreibt die technische Domäne oder Branche, für die eine CR entwickelt wird. In der analysierten Literatur wurden sieben Anwendungsbereiche identifiziert (siehe Abschnitt 4): ICT, ICS, Power Systems, CPS, IoT/IIoT, RAN & Mobile Devices sowie Intelligent Transportation Systems. ICT ist mit Abstand der am häufigsten dokumentierte Anwendungsbereich, gefolgt von ICS und Power Systems. Innerhalb der Anwendungsbereiche existieren zahlreiche Unterkategorien (Focus Areas), die für die Technologieauswahl jedoch von untergeordneter Relevanz sind.

6.4.3. Cyber Range Use Cases

Use Cases (siehe Abschnitt **??**) beschreiben konkrete Szenarien und Aktivitäten, die in einer CR durchgeführt werden. Sie sind jeweils einem oder mehreren Einsatzzwecken zugeordnet und bestimmen, welche Features und Technologien in der Target Infrastructure sowie in den Querschnittsbereichen benötigt werden.

> Die Wahl des Anwendungsbereichs ist ein zentraler Ausgangspunkt der Anforderungsanalyse und beeinflusst die Technologieauswahl insbesondere auf Ebene der Target Infrastructure und des Scenario-Bereichs.

6.5. Referenzarchitektur auf einen Blick

Die Referenzarchitektur (Abbildung 22) strukturiert die Technologien einer CR in vier vertikale Technologie-Layer sowie übergreifende Querschnittsbereiche. Sie wurde auf Basis der in Abschnitt 4.3 vorgestellten Ergebnisse sowie ergänzender Referenzarchitekturen aus der Literatur [71, 190, 209] entwickelt und dient in diesem Leitfaden als zentrales Strukturierungsinstrument für die Technologieauswahl.

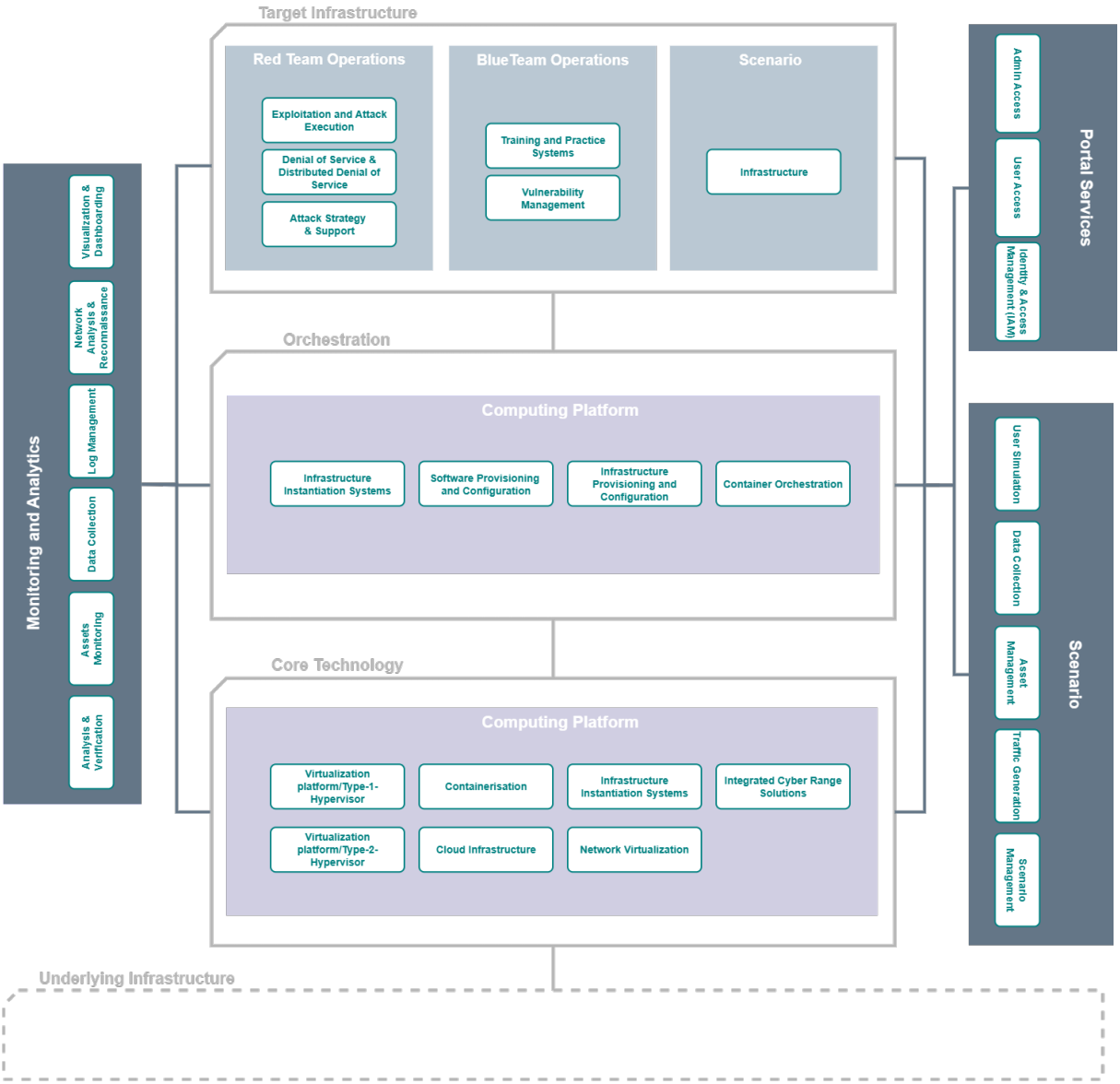


Abbildung 22: Referenzarchitektur für Cyber Ranges.

Die vier Layer sind hierarchisch angeordnet und bauen funktional aufeinander auf: Die Underlying Infrastructure stellt die physische Basis bereit, auf der die Core Technology aufsetzt. Der Orchestration Layer ermöglicht die automatisierte Verwaltung dieser technischen Ressourcen, und die Target Infrastructure bildet den operativen Kern der CR, in dem Übungen, Szenarien und Sicherheitsoperationen stattfinden.

Ergänzt werden die vier Layer durch Querschnittsbereiche, die sich funktional über mehrere oder alle Layer erstrecken: Monitoring & Analytics, Portal Services sowie Scenario. Diese Bereiche

sind nicht einem einzelnen Layer zugeordnet, sondern stellen layerübergreifende Funktionen und Features bereit.

Die detaillierte Beschreibung der Layer erfolgt in Abschnitt 6.6. Die Querschnittsbereiche sowie die Feature-Kategorien innerhalb aller Bereiche werden in Abschnitt 6.7 behandelt. Konkrete Technologien und Auswahlhilfen finden sich in Abschnitt 6.8.

6.6. Die vier Technologie-Layer

Die folgende Beschreibung erläutert Funktion, Abgrenzung und Relevanz jedes der vier Technologie-Layer. Die Layer bilden gemeinsam das strukturelle Rückgrat jeder CR-Implementierung. Ihre Ausprägung variiert je nach Zweck und Anwendungsbereich der CR erheblich, von minimalen Setups mit einem einzelnen Hypervisor bis hin zu komplexen, Cloud-basierten Plattformen mit vollautomatisierter Orchestrierung.

6.6.1. Underlying Infrastructure

Die Underlying Infrastructure bildet den untersten Layer der Referenzarchitektur und stellt die physische Grundlage dar, auf der alle weiteren Layer aufbauen. Sie umfasst die Hardware-Ressourcen, die für den Betrieb einer CR benötigt werden: physische Server, Netzwerkhardware (Switches, Router, Kabel und sonstige Verbindungskomponenten), Speichersysteme sowie Endgeräte wie Workstations oder spezialisierte Hardware für bestimmte Anwendungsbereiche.

In spezialisierten Anwendungsbereichen wie ICS oder CPS können auch physische Geräte Teil dieses Layers sein, die direkt an die CR-Umgebung angeschlossen werden. In der analysierten Literatur werden beispielsweise physische IEDs sowie RTDS-Hardware dokumentiert, die in HiL-Konfigurationen mit der virtuellen CR-Infrastruktur gekoppelt werden.

Als Alternative zur eigenen physischen Hardware kann die Underlying Infrastructure vollständig oder teilweise durch einen externen Cloud-Anbieter bereitgestellt werden. In diesem Fall übernimmt der Cloud-Provider die physische Infrastruktur als Managed Service, wodurch der initiale Investitionsaufwand entfällt und eine bedarfsgerechte Skalierung ermöglicht wird. Dies verlagert jedoch Fragen der Kontrolle, Datensouveränität und Netzwerklatenz an den Anbieter und ist daher im Rahmen der Anforderungsanalyse sorgfältig abzuwägen.

> Die Underlying Infrastructure ist nicht der primäre Scope dieses Leitfadens. Ihre Beschreibung dient dem Verständnis der Gesamtarchitektur. Konkrete Empfehlungen zur Hardware-Dimensionierung sind nicht Gegenstand dieses Dokuments.

6.6.2. Core Technology

Der Core Technology Layer umfasst die grundlegenden Softwaretechnologien, die zur Abstraktion und Nutzung der physischen Ressourcen eingesetzt werden. Er bildet die technologische Basis, auf der die gesamte CR-Umgebung, also ihre virtuellen Systeme, Netzwerke und Dienste, realisiert wird. Technologien auf dieser Ebene bestimmen maßgeblich, welche Art von Umgebungen in der CR abgebildet werden können, wie flexibel diese konfiguriert werden können und wie stark verschiedene Komponenten voneinander isoliert sind.

Im Mittelpunkt des Core Technology Layers stehen Technologien zur Virtualisierung und Containerisierung, über die physische Ressourcen in logische, voneinander getrennte Einheiten aufgeteilt werden. Ergänzt werden diese durch die Netzwerkinfrastruktur, die die Kommunikation zwischen

virtuellen und physischen Systemen ermöglicht und die Abbildung realistischer Netzwerktopologien erlaubt. In Cloud-basierten Setups kann dieser Layer vollständig oder in Teilen durch Cloud-Dienste realisiert werden, wobei die logische Struktur erhalten bleibt.

Die Entscheidungen auf dieser Ebene wirken sich direkt auf alle höheren Layer aus: Die gewählte Virtualisierungs- oder Container-Plattform beeinflusst, welche Orchestrierungswerkzeuge eingesetzt werden können, und die Netzwerkarchitektur bestimmt, welche Szenarien in der Target Infrastructure realistisch abgebildet werden können. Der Core Technology Layer sollte daher frühzeitig und auf Basis klar definierter Anforderungen konzipiert werden.

6.6.3. Orchestration

Der Orchestration Layer umfasst Technologien zur automatisierten Bereitstellung, Konfiguration und Verwaltung der CR-Infrastruktur und -Dienste. Er stellt das Bindeglied zwischen den Basisressourcen des Core Technology Layers und der operativen Zielumgebung der Target Infrastructure dar. Während die Core Technology die Grundlage schafft, übernimmt der Orchestration Layer deren bedarfsgerechte, reproduzierbare und skalierbare Nutzung.

Die Notwendigkeit einer dedizierten Orchestrierungsschicht ergibt sich unmittelbar aus den Betriebsanforderungen moderner CRs: Übungsumgebungen müssen kurzfristig auf- und abgebaut, konsistent reproduziert und an wechselnde Szenarien angepasst werden können. Bei einer größeren Anzahl bereitzustellender Systeme stößt manuelle Konfiguration schnell an praktische Grenzen. Ansätze wie IaC und automatisiertes Konfigurationsmanagement sind daher ein zentrales Merkmal professionell betriebener CR-Implementierungen.

In der Referenzarchitektur überschneidet sich die Computing Platform, also die Gesamtheit der Virtualisierungs- und Containertechnologien, mit dem Orchestration Layer, da viele Plattformen sowohl Basistechnologie als auch Orchestrierungsfunktionen bereitstellen. Diese Überlappung ist in der finalen Architekturdarstellung entsprechend visualisiert (Abbildung 22).

6.6.4. Target Infrastructure

Die Target Infrastructure ist der operativ-inhaltliche Kern einer CR. Sie umfasst alle Systeme, Dienste und Umgebungen, die für die Durchführung konkreter Übungen, Experimente, Tests und Angriffsszenarien konfiguriert und bereitgestellt werden. Im Gegensatz zu den darunterliegenden Layern, die generische Infrastruktur und Automatisierung bereitstellen, ist die Target Infrastructure direkt auf den jeweiligen Zweck der CR ausgerichtet: Sie definiert, was angegriffen, verteidigt, untersucht oder trainiert wird.

Ein wesentliches Merkmal der Target Infrastructure ist die Möglichkeit, mehrere Instanzen parallel zu betreiben. Eine einzelne Instanz der Target Infrastructure entspricht dabei konzeptuell einem TB, das eine in sich geschlossene, zweckgerichtete Umgebung darstellt. Eine CR kann je nach Anforderung ein oder mehrere solcher TBs gleichzeitig betreiben. So kann beispielsweise für jede teilnehmende Person oder Gruppe in einer Übung eine eigene, isolierte Zielinfrastruktur bereitgestellt werden. Dies ermöglicht eine unabhängige, störungsfreie Übungsdurchführung und ist ein zentrales Argument für den Einsatz der Orchestrierungsschicht, die eine solche parallele Instanziierung automatisiert ermöglicht.

6.7. Feature-Kategorien

Der folgende Abschnitt erläutert die Feature-Kategorien, die in der Referenzarchitektur den einzelnen Layern zugeordnet sind. Feature-Kategorien fassen funktional verwandte Fähigkeiten einer CR zusammen. Die Beschreibungen basieren auf den in Abschnitt 4.3 vorgestellten *Technology Domains* und beschränken sich hier auf eine funktionale Erläuterung. Konkrete Technologien und Auswahlhinweise folgen in Abschnitt 6.8.

6.7.1. Computing Platform

Die Computing Platform fasst alle Technologien zusammen, die zur Bereitstellung, Abstraktion und Verwaltung von Rechen- und Netzwerkressourcen in einer CR eingesetzt werden. Sie ist eine der am häufigsten dokumentierten Technologiekategorien in der analysierten Literatur (vgl. Abschnitt 4.3) und erstreckt sich in der Referenzarchitektur über den Core Technology Layer und den Orchestration Layer.

Den Kern der Computing Platform bilden Technologien zur Virtualisierung und Containerisierung, über die physische Ressourcen in isolierte, logische Einheiten aufgeteilt werden. Hypervisoren, sowohl Typ-1-Lösungen, die direkt auf der Hardware laufen, als auch Typ-2-Lösungen, die als Anwendung auf einem Betriebssystem betrieben werden, ermöglichen die Erstellung und Verwaltung virtueller Maschinen. Containerisierung bietet eine leichtgewichtigere Alternative, bei der Anwendungen in isolierten Einheiten mit gemeinsam genutztem Betriebssystemkern ausgeführt werden. Container Orchestration ergänzt die Containerisierung um automatisiertes Scheduling, Skalierung und Verwaltung von Container-Workloads und ist dem Orchestration Layer zugeordnet.

Auf der Automatisierungsseite ermöglichen Infrastructure Instantiation Systems die automatisierte, reproduzierbare Bereitstellung von Infrastrukturkomponenten, während Infrastructure Provisioning and Configuration sowie Software Provisioning and Configuration die anschließende Konfiguration von Systemen und Diensten übernehmen. Diese Werkzeuge sind in der Literatur weit verbreitet und bilden gemeinsam die Grundlage für eine automatisierte Bereitstellung vollständiger CR-Umgebungen.

Ergänzend dazu stehen zwei übergreifende Betriebsmodelle zur Verfügung: Cloud Infrastructure, entweder als selbst betriebene Plattform oder über externe Managed Cloud Provider, ermöglicht eine bedarfsgerechte Skalierung der CR-Ressourcen. Integrated Cyber Range Solutions bündeln mehrere Komponenten in einer vorkonfigurierten Plattform und reduzieren damit den Implementierungsaufwand, schränken jedoch die Flexibilität bei der Anpassung einzelner Komponenten ein. Network Virtualization schließlich erlaubt die softwarebasierte Abbildung beliebiger Netzwerktopologien.

6.7.2. Monitoring & Analytics

Monitoring & Analytics ist ein Querschnittsbereich, der sich über alle Layer der Referenzarchitektur erstreckt. Die zugehörigen Features werden nicht auf einen einzelnen Layer beschränkt, sondern kommen je nach Anwendungsfall auf der Ebene der Core Technology, der Orchestration oder der Target Infrastructure zum Einsatz. In der analysierten Literatur zählt dieser Bereich zu den am breitesten dokumentierten (siehe Abschnitt 4.3), wobei Analysis & Verification und Data Collection die häufigsten Subdomains darstellen.

Data Collection umfasst die Erfassung von Netzwerk-, System- und Anwendungsdaten aus der laufenden CR-Umgebung. Log Management stellt die zentrale Speicherung, Indexierung und

Durchsuchbarkeit von Logdaten aus verschiedenen Quellen sicher. Beide Features sind in der analysierten Literatur besonders häufig dokumentiert.

Network Analysis & Reconnaissance bezeichnet die Analyse von Netzwerkverkehr und -topologien, sowohl zur Überwachung des CR-Betriebs als auch als Feature innerhalb von Übungsszenarien. Analysis & Verification umfasst die weitergehende Auswertung gesammelter Daten, etwa zur Erkennung von Anomalien, zur Verifikation von Angriffsdetektionsmechanismen oder zur Bewertung des Übungsverlaufs. Assets Monitoring bezeichnet die kontinuierliche Überwachung einzelner Systemkomponenten hinsichtlich Verfügbarkeit und Ressourcenauslastung, ist in der Literatur jedoch vergleichsweise selten explizit dokumentiert.

Visualization & Dashboarding macht die gesammelten und analysierten Daten für Betreibende und Teilnehmende zugänglich. Dashboards werden in CRs sowohl für den technischen Betrieb als auch im Ausbildungskontext eingesetzt, etwa um Teilnehmenden Echtzeit-Feedback über den Verlauf einer Übung zu geben.

6.7.3. Portal Services

Portal Services ist ein Querschnittsbereich, der den kontrollierten Zugang zur CR-Umgebung für verschiedene Nutzergruppen bereitstellt und verwaltet. In der analysierten Literatur dominiert User Access mit deutlichem Abstand als häufigste Subdomain, gefolgt von Admin Access. IAM ist vergleichsweise selten explizit dokumentiert (siehe Abschnitt 4.3).

User Access bezeichnet die Bereitstellung einer Zugangsoberfläche für Teilnehmende einer Übung. Über webbasierte Portale erhalten Nutzende Zugang zu ihrer Übungsumgebung, zu Aufgabenstellungen und zu Feedback- oder Bewertungsfunktionen. Admin Access adressiert den gesicherten Fernzugriff für Betreibende und Administrator*innen auf alle Systemkomponenten der CR, etwa zur Konfiguration, Überwachung oder zum Eingreifen während einer laufenden Übung.

IAM umfasst die Verwaltung von Benutzeridentitäten, Rollen und Zugriffsrechten innerhalb der CR. Es stellt sicher, dass Teilnehmende, Instruktor*innen und Administrator*innen jeweils nur auf jene Ressourcen zugreifen können, die ihrer Rolle entsprechen. MFA ist in der analysierten Literatur als Bestandteil des Zugangsmanagements dokumentiert.

6.7.4. Scenario

Scenario ist ein Querschnittsbereich, der Technologien zur Unterstützung der Erstellung, Durchführung und Steuerung von Übungsszenarien zusammenfasst. Innerhalb der Target Infrastructure findet sich die Scenario Infrastructure, die jene Infrastrukturkomponenten beschreibt, die für konkrete Szenarien benötigt werden, darunter auch Werkzeuge zur Simulation von Benutzeraktivitäten und -verhalten. Darüber hinaus kommen Szenariotechnologien auch im Core Technology Layer zum Einsatz, insbesondere zur Emulation und Simulation von Geräten und physischen Systemen. Dies ist besonders in Anwendungsbereichen wie CPS, ICS, Power Systems und Intelligent Transportation Systems ausgeprägt, wo reale Hardware durch Software-Simulatoren nachgebildet wird.

Data Collection bezeichnet im Kontext dieses Querschnittsbereichs die szenariobezogene Erfassung von Ereignissen, Aktionen und Metriken während einer laufenden Übung, etwa Nutzeraktionen, Systemzustände oder Angriffsereignisse. Diese Daten bilden die Grundlage für Auswertung und Nachbesprechung. Die explizite Zuordnung von Data Collection zum Scenario-Bereich basiert auf anderen einschlägigen Referenzarchitekturen, in denen die Datenerfassung als integraler Bestandteil des Szenariobetriebs beschrieben wird. Traffic Generation umfasst die automatisierte

Erzeugung von Netzwerkverkehr innerhalb von Szenarien, sowohl legitimen als auch bösartigen, um realistische Netzwerkbedingungen für Übungen herzustellen.

User Simulation bezeichnet die automatisierte Nachbildung von Nutzeraktivitäten in der CR-Umgebung, beispielsweise durch skriptgesteuerte Browser-Interaktionen. Sie dient dazu, realistisches Nutzerverhalten in Szenarien abzubilden, ohne dass reale Personen diese Rollen übernehmen müssen. Asset Management umfasst die Verwaltung und Inventarisierung aller Ressourcen innerhalb eines Szenarios oder der gesamten CR-Umgebung.

Scenario Management fasst Funktionen zur Erstellung, Verwaltung, Durchführung und Auswertung von Übungsszenarien zusammen. Dieser Bereich ist in der zugrundeliegenden Literaturstudie (Abschnitt 4.3) nicht als eigenständige Architekturkomponente ausgewiesen, findet sich jedoch in anderen einschlägigen Referenzarchitekturen [71, 190, 209] als essenzieller Bestandteil einer CR. Er wurde daher in die vorliegende Referenzarchitektur aufgenommen, um den vollständigen Lebenszyklus eines Szenarios, von der Definition über die Durchführung bis zur Nachbereitung, abzudecken.

6.7.5. Feature-Kategorien im Target Infrastructure Layer

Die Target Infrastructure ist jener Layer der Referenzarchitektur, der in der analysierten Literatur die größte Vielfalt an Technologien und Feature-Kategorien aufweist. Für die Bereiche Red Team Operations und Scenario finden sich zahlreiche Nennungen über nahezu alle Use Cases hinweg. Hinzu kommen Bereiche wie Blue Team Operations, Data Storage, Custom Development und weitere, die je nach Anwendungsfall unterschiedlich ausgeprägt sind. Die nachfolgenden Beschreibungen umfassen daher nur eine Auswahl häufig dokumentierter Feature-Kategorien. Eine vollständige Übersicht aller identifizierten Feature-Kategorien und Technologien findet sich in Abschnitt 4.3.

Red Team Operations umfasst Technologien zur Simulation von Angreifenden und zur Durchführung offensiver Sicherheitsoperationen. Es ist in der analysierten Literatur der am breitesten dokumentierte Technologiebereich innerhalb der Target Infrastructure, mit Nennungen quer durch alle untersuchten Anwendungsbereiche. Network Scanning & Reconnaissance, eine der häufigsten Subdomains insgesamt, dient der systematischen Erkundung von Zielnetzwerken und -systemen als Vorbereitung für Angriffe. Exploitation and Attack Execution umfasst Werkzeuge zur Ausnutzung von Schwachstellen und zur Durchführung konkreter Angriffe. Attack Strategy & Support beinhaltet Frameworks und Methoden zur strukturierten Planung und Ausführung von Angriffskampagnen, darunter taktik- und technikbasierte Ansätze. Denial of Service & Distributed Denial of Service bezeichnet Werkzeuge zur gezielten Überlastung von Systemen und Netzwerken, die insbesondere in ICS-, IoT- und ICT-Umgebungen dokumentiert sind.

Blue Team Operations fasst Technologien für Verteidigung, Detektion und Reaktion auf Angriffe zusammen. Intrusion Detection & Prevention (IDS/IPS) ist die am häufigsten dokumentierte Subdomain in diesem Bereich und findet sich in vielen Anwendungsbereichen. SIEM & Security Analytics bezeichnet Plattformen zur zentralen Aggregation, Korrelation und Analyse von Sicherheitsereignissen aus verschiedenen Quellen. Vulnerability Management umfasst Werkzeuge zur systematischen Identifikation und Bewertung von Schwachstellen in der Zielinfrastruktur. Training and Practice Systems bezeichnet dedizierte Lern- und Übungsumgebungen, in denen defensive Fähigkeiten praxisnah trainiert werden können.

Scenario Infrastructure beschreibt innerhalb der Target Infrastructure jene Komponenten, die für die Realisierung konkreter Übungsszenarien benötigt werden. Infrastructure ist mit Abstand die häufigste Subdomain im gesamten Scenario-Bereich und umfasst die Systeme, Dienste und Protokolle, die das Zielszenario inhaltlich ausmachen, von Webservern und Datenbanken über

industrielle Steuerungssysteme bis hin zu spezialisierten Protokollimplementierungen. Werkzeuge zur Simulation von Nutzeraktivitäten und -verhalten sind ebenfalls in der Target Infrastructure verortet, wenngleich sie in der analysierten Literatur selten explizit dokumentiert sind.

Integrated Testbed Solutions sind vorkonfigurierte Plattformen, die eine vollständige Zielinfrastruktur als integrierte Lösung bereitstellen. In anderen einschlägigen Referenzarchitekturen werden solche Lösungen häufig als fertige Target Infrastructure beschrieben. Obwohl in der analysierten Literatur vergleichsweise selten dokumentiert, sind sie für die Technologieauswahl relevant, da sie die Erstellung vollständiger Zielinfrastrukturen mit erheblich reduziertem Implementierungsaufwand ermöglichen. Sie eignen sich besonders für spezialisierte Anwendungsbereiche wie CPS, ICS oder Telekommunikation, für die dedizierte Plattformen verfügbar sind.

6.8. Technologieauswahl

Die Auswahl geeigneter Technologien für eine CR ist kein isolierter Schritt, sondern ein strukturierter Prozess (Abbildung 23), der auf den zuvor definierten Anforderungen aufbaut. Der folgende Leitfaden gliedert diesen Prozess in vier Phasen, wobei die Entscheidungen der frühen Phasen die Optionen der späteren Phasen direkt beeinflussen. Die Reihenfolge ist als Empfehlung zu verstehen: In der Praxis können einzelne Phasen iterativ durchlaufen oder parallel bearbeitet werden.

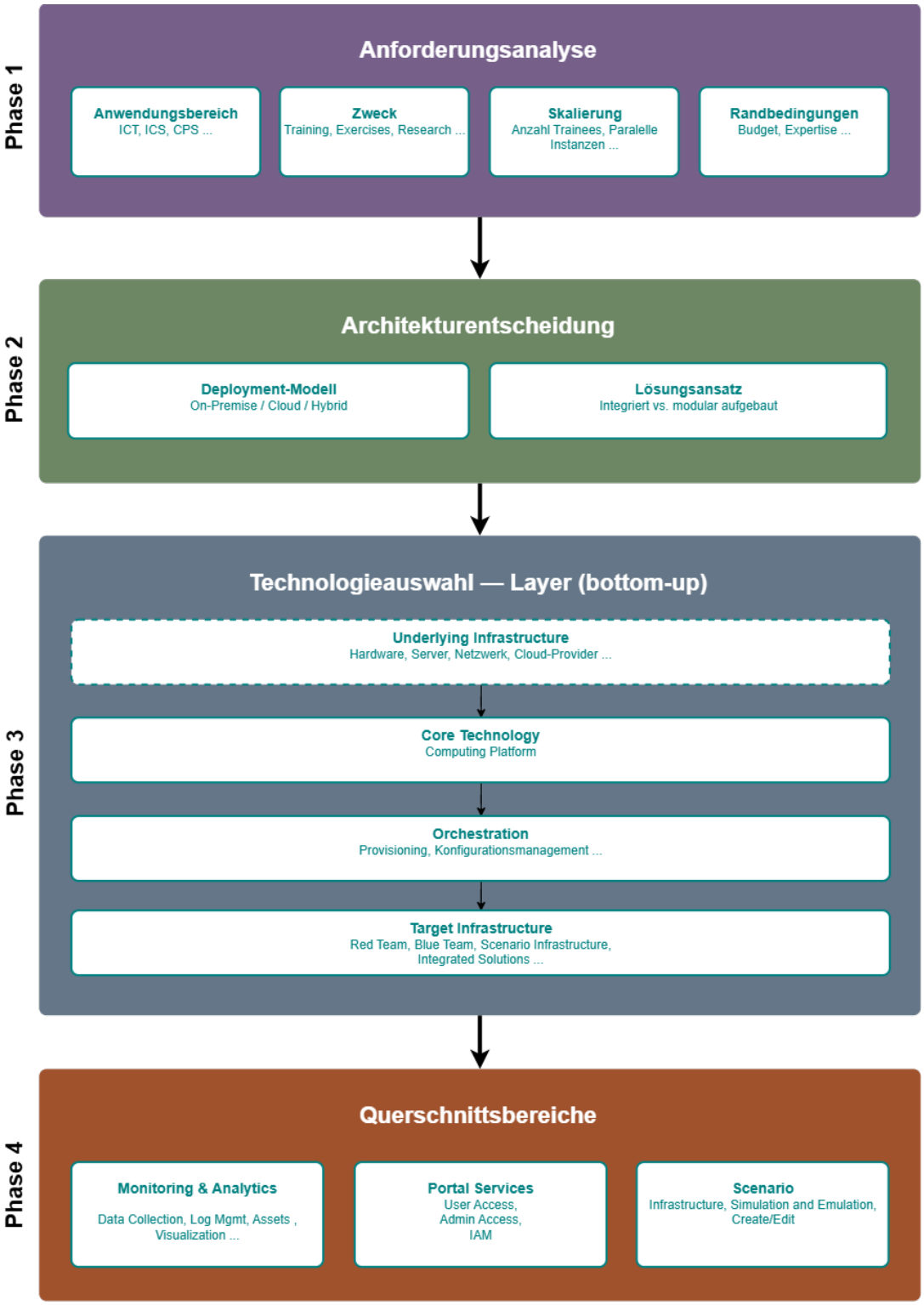


Abbildung 23: Leitfaden zur Technologieauswahl für Cyber Ranges.

6.8.1. Phase 1: Anforderungsanalyse

Die Anforderungsanalyse bildet die Grundlage aller weiteren Entscheidungen. Sie beantwortet die Frage, wofür die CR gebaut wird, für wen sie betrieben wird und unter welchen Rahmenbedingungen dies geschieht.

Einsatzzweck

Der Einsatzzweck beeinflusst, welche Feature-Kategorien empfohlen werden. Eine CR für Training and Exercises oder Education erfordert andere Schwerpunkte als eine Plattform für Research, Testing and Experimentation.

Research, Testing and Experimentation

Im Fokus stehen reproduzierbare und gut instrumentierte Umgebungen. Dieser Einsatzzweck stellt besondere Anforderungen an die Messbarkeit und Nachvollziehbarkeit von Experimenten, ohne dass bestimmte Feature-Kategorien pauschal als relevanter eingestuft werden können. Die konkreten technologischen Schwerpunkte hängen stark vom jeweiligen Forschungsthema ab, weshalb an dieser Stelle keine Beispieltechnologien angeführt werden.

Training and Exercises

Im Vordergrund stehen realistische Übungsumgebungen sowie Werkzeuge zur Begleitung und Bewertung von Teilnehmenden. Empfohlen werden Technologien aus den Bereichen Learning Management sowie User Management, da diese die Organisation von Übungen, die Verwaltung von Teilnehmenden und die Auswertung von Lernfortschritten unterstützen.

Beispieltechnologien:

- Moodle: In der analysierten Literatur häufig dokumentiertes Lernmanagementsystem, das in CR-Umgebungen für die Verwaltung von Aufgaben, Bewertungen und Lernressourcen eingesetzt wird.
- Windows Active Directory: In mehreren dokumentierten Implementierungen zur zentralen Nutzerverwaltung und Authentifizierung eingesetzt.

Education

Ähnlich wie bei Training and Exercises sind Lernmanagementsysteme und Bewertungswerkzeuge empfohlen. Zusätzlich gewinnen Werkzeuge zur didaktischen Gestaltung von Szenarien an Bedeutung. Der Einsatzzweck Education findet sich in der analysierten Literatur vorwiegend in ICT-Umgebungen.

Beispieltechnologien:

- Moodle: Wird auch im Education-Kontext eingesetzt, kombiniert mit Bewertungs- und Feedbackmechanismen.
- Bazaar Collaborative Learning Environment: in der Literatur dokumentierte Plattform, die kollaboratives Lernen und technische Simulation in CR-Umgebungen kombiniert.

Use Cases

Use Cases (siehe Kapitel 4.2) konkretisieren den Einsatzzweck und legen fest, welche Features in der Target Infrastructure und im Scenario-Bereich benötigt werden. Nachfolgend werden ausgewählte Use Cases beschrieben.

Capture the Flag (CTF)

CTF-Szenarien erfordern eine strukturierte Übungsplattform mit definierten Aufgaben und automatischer Auswertung sowie eine isolierte Zielinfrastruktur.

Beispieltechnologien:

- CTFd: In der Literatur dokumentierte Plattform zur Verwaltung von CTF-Wettbewerben, die Aufgabenmanagement, Scoreboard und Teilnehmendenverwaltung in einer integrierten Lösung bereitstellt.

Red Team vs. Blue Team

Dieser Anwendungsfall erfordert sowohl offensive Werkzeuge (Red Team Operations) als auch defensive Technologien (Blue Team Operations) sowie eine realistische Zielinfrastruktur.

Beispieltechnologien:

- Metasploit: Framework für Penetrationstests und Exploit-Ausführung, das in zahlreichen analysierten Implementierungen als zentrales Angriffswerkzeug eingesetzt wird.
- Suricata: Netzwerkbasiertes IDS/IPS, das häufig auf der Verteidigungsseite dokumentiert wird.

Cyber Security Training (allgemein)

Für allgemeines Cybersicherheitstraining werden breite Toolsets benötigt, die verschiedene Angriffsszenarien und Verteidigungsmaßnahmen abdecken.

Beispieltechnologien:

- NETLAB+: Plattform für virtualisierte Lab-Umgebungen, die in Bildungseinrichtungen für praxisnahes Cybersicherheitstraining eingesetzt wird.

Anwendungsbereich

Der Anwendungsbereich legt fest, welche technische Domäne in der CR abgebildet wird. Er beeinflusst insbesondere die Auswahl von Technologien in der Target Infrastructure und im Scenario-Bereich.

ICT

Im ICT-Bereich steht die Abbildung typischer IT-Infrastrukturen im Vordergrund. Die Technologieauswahl ist hier am breitesten, da nahezu alle dokumentierten Feature-Kategorien relevant sein können. Für diesen Anwendungsbereich sind keine spezifischen Technologieempfehlungen abseits der allgemeinen Layer-Auswahl in Phase 3 erforderlich.

ICS, CPS und Power Systems

In diesen Bereichen müssen physische Geräte wie speicherprogrammierbare Steuerungen, Feldgeräte oder Energiemanagementsysteme durch Software-Simulatoren nachgebildet werden. Empfohlen werden Technologien aus der Kategorie Simulation and Emulation, die in der analysierten Literatur in diesen Anwendungsbereichen besonders häufig dokumentiert sind.

Beispieltechnologien:

- MATLAB/Simulink: Die in der analysierten Literatur am häufigsten dokumentierte Simulationsumgebung für physische Systeme in CR-Umgebungen. Wird für die Modellierung von Energienetzen, industriellen Steuerungssystemen und cyber-physischen Infrastrukturen eingesetzt.
- OPAL-RT: Echtzeit-Digitalsimulator, der in mehreren analysierten Implementierungen für die hardwareintegrierende Simulation von Energiesystemen und industriellen Steuerungsprozessen eingesetzt wird.

RAN und Mobile Devices (5G)

Für CRs in diesem Bereich werden spezialisierte Werkzeuge zur Simulation von Mobilfunknetzinfrastrukturen empfohlen, da reale 5G-Kernnetzkomponenten in der CR-Umgebung softwarebasiert nachgebildet werden müssen.

Beispieltechnologien:

- Free5GC: In der analysierten Literatur dokumentierte Open-Source-Implementierung eines 5G-Kernnetzwerks, die in CR-Umgebungen zur Simulation von 5G-Netzinfrastrukturen eingesetzt wird.
- NSF POWDER Wireless Platform: In der analysierten Literatur dokumentierte Forschungsplattform für drahtlose Netzwerke, die speziell für Experimente mit 5G-Funktechnologien konzipiert ist.

Randbedingungen

Randbedingungen leiten die Technologieauswahl unabhängig vom fachlichen Bedarf. Budget beeinflusst die Entscheidung zwischen kommerziellen und Open-Source-Lösungen. Die analysierten Implementierungen zeigen eine deutliche Dominanz von Open-Source-Technologien wie Docker, Ansible und OpenStack, was auf deren Verbreitung auch in ressourcenbeschränkten Umgebungen hindeutet. Verfügbare Expertise beeinflusst die Komplexität der einsetzbaren Lösungen, da Technologien wie Terraform oder Kubernetes spezialisiertes Wissen erfordern. Compliance-Anforderungen können den Einsatz bestimmter Cloud-Dienste einschränken oder On-Premise-Lösungen erfordern.

Skalierung

Die Anzahl der gleichzeitig betriebenen Target-Infrastructure-Instanzen hat direkte Auswirkungen auf die Wahl der Computing Platform und der Orchestrierungsschicht. Für kleine Umgebungen mit wenigen parallelen Instanzen kann eine einfache, Hypervisor-basierte Lösung ausreichen. Bei größeren Umgebungen mit vielen gleichzeitigen Teilnehmenden empfiehlt sich eine containerbasierte Architektur mit Orchestrierung, da diese eine automatisierte, ressourceneffiziente parallele Bereitstellung ermöglicht.

6.8.2. Phase 2: Architekturentscheidung

Die Architekturentscheidung legt das grundlegende Betriebsmodell der CR fest. Sie beeinflusst direkt, welche Technologien in Phase 3 zur Verfügung stehen.

Deployment-Modell

On-Premise

Die gesamte Infrastruktur wird selbst betrieben. Dieses Modell bietet volle Kontrolle über Daten und Netzwerk, erfordert jedoch eigene Hardware und Betriebskapazitäten.

Beispieltechnologien:

- OpenStack: Die in der analysierten Literatur am häufigsten dokumentierte Plattform für selbst betriebene Cloud-Infrastrukturen in CR-Umgebungen. Ermöglicht die Bereitstellung einer privaten Cloud mit vollständiger Kontrolle über Rechenressourcen, Netzwerke und Speicher.
- VMware vSphere: Weit verbreitete kommerzielle Virtualisierungsplattform, die in mehreren analysierten Implementierungen als Basis für große CR-Umgebungen eingesetzt wird.

Cloud (Managed Provider)

Rechenressourcen werden bei einem externen Anbieter bezogen. Dieses Modell reduziert den initialen Investitions- und Betriebsaufwand und ermöglicht flexible Skalierung.

Beispieltechnologien:

- AWS und Microsoft Azure: In der analysierten Literatur dokumentierte Cloud-Plattformen für CR-Implementierungen, insbesondere wenn Skalierbarkeit oder geografische Verteilung erforderlich ist.

Hybrid

Eine Kombination aus On-Premise- und Cloud-Ressourcen. Dieses Modell erlaubt es, sensible oder latenzempfindliche Komponenten lokal zu betreiben und gleichzeitig die Skalierungsvorteile der Cloud zu nutzen.

Lösungsansatz

Integrierte Lösung

Eine vorkonfigurierte Plattform integriert mehrere Layer der CR-Architektur. Dieser Ansatz reduziert den Implementierungsaufwand erheblich, schränkt jedoch die Flexibilität bei der Anpassung einzelner Komponenten ein.

Beispieltechnologien:

- KYPO: Dokumentierte Open-Source-Plattform für CRs, die Computing Platform, Orchestrierung und Teile der Target Infrastructure integriert.
- EDURange: Cloudbasierte CR-Plattform, die insbesondere für Ausbildungszwecke konzipiert ist und vorkonfigurierte Sicherheitsübungen bereitstellt.

Modularer Aufbau

Einzelne Technologien werden gezielt für spezifische Feature-Kategorien ausgewählt und zu einer Gesamtlösung zusammengestellt. Dieser Ansatz bietet maximale Flexibilität, erfordert jedoch höheres technisches Wissen und mehr Integrationsaufwand. Er ist besonders dann sinnvoll, wenn spezifische Anforderungen nicht durch verfügbare integrierte Lösungen abgedeckt werden.

6.8.3. Phase 3: Technologieauswahl nach Layer

Die Technologieauswahl erfolgt von unten nach oben, da Entscheidungen auf niedrigeren Layern die verfügbaren Optionen auf höheren einschränken. Die in Phase 1 und Phase 2 getroffenen Entscheidungen fließen direkt in die Auswahl auf jedem Layer ein.

Core Technology

Die Wahl der Computing Platform ist eine der folgenreichsten Entscheidungen im gesamten Prozess, da sie die Orchestrierungswerkzeuge und die möglichen Skalierungsszenarien direkt beeinflusst.

Beispieltechnologien:

- Proxmox VE: Open-Source-Typ-1-Virtualisierungsplattform, die sowohl KVM-basierte virtuelle Maschinen als auch Container-Virtualisierung unterstützt und in CR-Implementierungen aufgrund ihrer kostenlosen Verfügbarkeit dokumentiert ist.
- KVM: Im Linux-Kernel integrierter Hypervisor, der in zahlreichen analysierten Implementierungen als Basis für virtuelle Maschinen eingesetzt wird.
- Docker: Die in der analysierten Literatur mit Abstand am häufigsten dokumentierte Containerisierungslösung für CR-Umgebungen.
- Kubernetes: Plattform zur Container-Orchestrierung, die in größeren CR-Umgebungen für automatisches Scheduling und Skalierung von Container-Workloads eingesetzt wird.
- Mininet: Netzwerksimulator, der die Erstellung virtueller Netzwerktopologien auf einem einzelnen Rechner ermöglicht und in CR-Umgebungen für die Simulation von SDN-Netzwerken eingesetzt wird.

Orchestration

Die Auswahl der Orchestrierungswerkzeuge hängt von der gewählten Computing Platform und vom Automatisierungsgrad der CR ab. Für größere Umgebungen oder solche mit häufig wechselnden Szenarien ist eine vollständige Automatisierung der Bereitstellung empfehlenswert.

Beispieltechnologien:

- Terraform: IaC-Werkzeug, das die automatisierte Bereitstellung von Infrastrukturkomponenten ermöglicht und in CR-Umgebungen häufig für die Bereitstellung vollständiger Übungsumgebungen eingesetzt wird.
- Ansible: Das in der analysierten Literatur am häufigsten dokumentierte Konfigurationsmanagement-Werkzeug für CR-Umgebungen. Ermöglicht die agentenlose, automatisierte Konfiguration von Systemen und Diensten über YAML-basierte Playbooks.

Target Infrastructure

Die Technologieauswahl in der Target Infrastructure wird stärker als jeder andere Layer durch den Anwendungsbereich und die Use Case aus Phase 1 bestimmt. Die folgenden Empfehlungen sind daher als Ausgangspunkte zu verstehen, die je nach konkretem Bedarf angepasst werden müssen.

Red Team Operations

Beispieltechnologien:

- Metasploit: Framework für Penetrationstests mit umfangreicher Bibliothek an Exploits und Payloads. In der analysierten Literatur das am häufigsten genannte Werkzeug für Exploitation and Attack Execution.
- Nmap: Werkzeug für Netzwerk-Scanning und Reconnaissance, das in CR-Szenarien zur Erkundung von Zielnetzwerken eingesetzt wird.

- MITRE Caldera: Framework zur Adversary Emulation, das automatisierte Angriffskampagnen auf Basis des MITRE-ATT&CK-Frameworks ermöglicht.

Blue Team Operations

Beispieltechnologien:

- Suricata: Leistungsfähiges Open-Source-IDS/IPS, das in der analysierten Literatur eines der am häufigsten dokumentierten Intrusion-Detection-Systeme in CR-Umgebungen darstellt.
- ELK Stack (Elasticsearch, Logstash, Kibana): In mehreren analysierten Implementierungen als integrierte Lösung für Log Management, Suche und Visualisierung von Sicherheitsereignissen eingesetzt.
- OpenVAS: Open-Source-Werkzeug für Vulnerability Management, das in CR-Umgebungen zur systematischen Identifikation von Schwachstellen in der Zielinfrastruktur eingesetzt wird.

Scenario Infrastructure

Die Auswahl ist stark vom Anwendungsbereich abhängig. Im ICT-Bereich werden häufig Standard-Webserver, Datenbanken und Betriebssystem-Images als Zielobjekte eingesetzt. Für ICS- und CPS-Umgebungen sind spezialisierte Simulationskomponenten erforderlich.

Beispieltechnologien:

- EXata CPS: Ermöglicht die Simulation von cyber-physischen Infrastrukturen inklusive industrieller Kommunikationsprotokolle und wird in mehreren Implementierungen für ICS- und Power-Systems-Szenarien dokumentiert.

6.8.4. Phase 4: Querschnittsbereiche

Die Technologien der Querschnittsbereiche sind in der Regel unabhängig vom Anwendungsbereich, werden jedoch in ihrer Ausprägung vom Einsatzzweck beeinflusst.

Monitoring & Analytics

Beispieltechnologien:

- Prometheus: Weit verbreitetes Open-Source-Monitoring-System für die Erfassung von Zeitreihendaten aus verschiedenen Quellen. In CR-Umgebungen für das Infrastruktur-Monitoring eingesetzt.
- Grafana: Visualisierungsplattform, die in Kombination mit Prometheus oder dem ELK Stack Dashboards für den Betrieb sowie für Teilnehmende in Übungen bereitstellt.
- Wireshark: Werkzeug zur Netzwerkverkehrsanalyse, das in CR-Umgebungen sowohl für den Betrieb als auch als Übungswerkzeug in Trainingsszenarien dokumentiert wird.

Portal Services

Beispieltechnologien:

- Apache Guacamole: Browserbasierte Remote-Desktop-Lösung, die in mehreren analysierten Implementierungen eingesetzt wird, um Teilnehmenden und Administrierenden über eine gesicherte Weboberfläche Zugang zu CR-Ressourcen zu ermöglichen.

- OpenSSH: in CR-Umgebungen als Standard für den administrativen Fernzugriff auf Systemkomponenten dokumentiert.
- Authentik: Identity Provider, der MFA und zentrales Zugriffsmanagement für CR-Umgebungen bereitstellt.

Scenario

Beispieltechnologien:

- Selenium: Wird in der analysierten Literatur zur Simulation von Nutzeraktivitäten eingesetzt, indem Browser-Interaktionen automatisiert werden und so realistische Nutzeraktivitätsmuster erzeugt werden.
- curl-loader: Werkzeug zur Generierung von HTTP-Netzwerkverkehr, das in CR-Szenarien zur Erzeugung realistischer oder bösartiger Netzwerklast eingesetzt wird.

6.9. Hinweise zur Anwendung

Die in diesem Leitfaden beschriebene Technologieauswahl ist kein einmaliger Prozess. CRs werden typischerweise über längere Zeiträume betrieben und weiterentwickelt, und die Technologielandschaft in diesem Bereich unterliegt einem stetigen Wandel. Die hier vorgestellten Empfehlungen und Beispieltechnologien spiegeln den Stand der analysierten Literatur (Abschnitt 3) wider und sind entsprechend als Orientierungspunkte zu verstehen, nicht als abschließende Vorgaben.

In der Praxis wird die Technologieauswahl häufig iterativ erfolgen: Erste Entscheidungen auf Layer-Ebene schaffen Erfahrungswerte, die spätere Anpassungen informieren. Auch Änderungen im Anwendungsbereich, im Einsatzzweck oder in den Randbedingungen können eine Überprüfung und Anpassung der gewählten Technologien erforderlich machen. Es empfiehlt sich daher, die getroffenen Auswahlentscheidungen zu dokumentieren und in regelmäßigen Abständen zu evaluieren.

7. Zukünftige Arbeiten

Das folgende Kapitel behandelt Aspekte, die zukünftige Übersichtsarbeiten basierend auf der vorliegenden systematischen Literaturübersicht adressieren sollten. Darüber hinaus zeigt der Abschnitt zukünftige Trends im Zusammenhang mit dem Aufkommen von AI auf.

7.1. Taxonomische Harmonisierung und semantische Formalisierung

Die in der Diskussion in Kaptel 5 identifizierten Herausforderungen hinsichtlich Taxonomien und logischer Architekturen deuten nicht nur auf eine bestehende Forschungslücke hin, sondern unterstreichen auch die Notwendigkeit einer gemeinsamen konzeptuellen Grundlage in diesem Bereich. Vor diesem Hintergrund erscheint es essenziell, dass zukünftige Arbeiten bestehende Taxonomien und Architekturen systematisch weiterentwickeln und diese konsistent auf etablierte architektonische Beschreibungen, Dokumentationen und taxonomische Rahmenwerke anwenden. Eine solche Harmonisierung kann die Planung, das Design und die Klassifikation von CRs und TBs erheblich erleichtern und darüber hinaus die gezielte Weiterentwicklung von CRs und TBs hinsichtlich ihrer Architektur, Funktionalität und Integration unterstützen.

Die im Verlauf dieser Übersichtsarbeit identifizierte heterogene Terminologie und architektonische Darstellung legen nahe, dass Reproduzierbarkeit und Vergleichbarkeit bei CR- und TB-Implementierungen nicht allein durch prozedurales Tooling erreicht werden können. Ontologiebasierte Ansätze stellen eine vielversprechende Richtung für die Etablierung einer solchen Grundlage dar. Wen et al. [204] schlagen eine RDF/OWL-basierte Ontologie zur Modellierung von Cybersicherheits-Übungsszenarien vor, die eine gemeinsame semantische Struktur bereitstellt, welche das Teilen und die Wiederverwendung von Szenariowissen über Anwendungen und Community-Grenzen hinweg ermöglicht. Darauf aufbauend schlagen Kampourakis et al. [73] ein breiteres ontologiebasiertes Framework vor, das die strukturellen, funktionalen, informationellen und entscheidungsbezogenen Aspekte des gesamten CR-Ökosystems in einem maschinell interpretierbaren, in OWL 2 DL implementierten Modell formalisiert und damit Konsistenzprüfung, automatisiertes Schlussfolgern und Nachvollziehbarkeit über Abstraktionsebenen hinweg ermöglicht. Die Autor*innen charakterisieren dieses Framework als semantisches Metamodell über architektonisches Wissen, das genau die Art terminologischer und repräsentationeller Heterogenität adressiert, die in dieser Übersichtsarbeit identifiziert wurde. Die hier zusammengestellte strukturierte Datengrundlage, die Technologien, Use Cases und Architektur-Layer über 199 Publikationen hinweg konsolidiert, kann als empirische Grundlage für solche Formalisierungsbemühungen dienen, und zukünftige Arbeiten könnten darauf aufbauen, um gemeinsame, semantisch fundierte Repräsentationen der CR- und TB-Domäne zu entwickeln.

Hinsichtlich der Methodik dieser Arbeit lässt die semantische Zusammenfassung und Kategorisierung von Technologien einen vergleichsweise großen interpretativen Spielraum zu. Ein stärker strukturierter Ansatz, der auf qualitativer Analyse und der expliziten Identifikation einzelner technologischer Funktionen beruht, erscheint methodisch letztlich geeigneter, da diese Funktionen die Merkmale von CRs und TBs bilden. Zukünftige Forschung könnte einzelne Komponenten dieser Arbeit eingehender untersuchen und qualitativ bewerten, um eine alternative Kategorisierung und Strukturierung abzuleiten, die präziser und besser an den jeweiligen Kontext angepasst ist.

7.2. Generative AI und große Sprachmodelle

Eine weitere Entwicklungslinie betrifft die Integration generativer AI und Large Language Models (LLMs) in CR- und TB-Implementierungen. Die in dieser Übersichtsarbeit identifizierten AI- und

ML-Technologien werden überwiegend für Erkennungs- und Analyseaufgaben eingesetzt, etwa Anomalieerkennung und das Training von Intrusion-Detection-Modellen. Generative AI stellt eine qualitativ andere Richtung dar: Zacharis und Patsakis [213] schlagen ein ML-gestütztes Framework zur automatisierten Generierung von Cyber-Übungsinhalten mittels Named Entity Recognition und einer dedizierten Szenario-Ontologie vor, während Palumickas et al. [129] einen generativen AI-Prototyp für dynamische, interaktive Szenariogenerierung evaluieren und dabei sowohl dessen Potenzial als auch aktuelle Einschränkungen hinsichtlich Konsistenz und Wiederholbarkeit aufzeigen. Yamin et al. [210] untersuchen den Einsatz von LLMs als aktive Teilnehmende in Übungssimulationen statt lediglich als Werkzeug zur Szenarioerstellung, und Kampourakis et al. [72] demonstrieren den Einsatz LLM-gestützten Expertenschlussfolgerns zur Unterstützung strukturierter CR-Evaluierung. Berg et al. [15] zeigen, dass LLMs die Generierung lauffähiger ICS-Simulationen aus Klartextbeschreibungen automatisieren können, wobei funktionierende Testbeds in unter 90 Sekunden entstehen, und argumentieren, dass solche Prompt-zu-Simulation-Pipelines gut für CRs, Deception-Systeme und schnelles Prototyping geeignet sind, auch wenn die generierten Modelle nicht für hochpräzise Simulationen geeignet sind. Da diese Arbeiten größtenteils nach dem in dieser Übersichtsarbeit untersuchten Korpus erschienen sind, stellt die systematische Integration generativer AI in CR- und TB-Workflows, einschließlich Szenariogenerierung, automatisiertem Red Teaming und Plattformevaluierung, eine bedeutende aufkommende Entwicklungslinie für zukünftige Forschung dar.

7.3. Weitere Plattformen und Aspekte für gezielte Übersichtsarbeiten

Der systematische Umfang dieser Übersichtsarbeit bedeutet, dass mehrere in der Literatur dokumentierte, repräsentative Plattformen außerhalb des analysierten Korpus liegen. Sipola et al. [169] beschreiben einen Digital Twin einer Lebensmittel-Lieferkette, der auf der von der JAMK University of Applied Sciences betriebenen Plattform Realistic Global Cyber Environment (RGCE) bereitgestellt wird, und demonstrieren dessen Einsatz in einer Live-Cyber-Übung zur Schulung von Organisationen in Lieferketten-Cybersicherheit. Bonagura et al. [26] stellen das Testbed Hydra vor, das ein reales Wasserverteilungssystem emuliert und zur Generierung des HydraCPS-Datensatzes zur Evaluierung von Intrusion-Detection-Systemen unter simulierten cyber-physischen Angriffen auf kritische Infrastruktur eingesetzt wird. Cruz und Simões [42] beschreiben ein flexibles Framework zur Erstellung von Labor- und ICS-Cyber-Range-Umgebungen für Trainingszwecke, angewendet im Kontext eines Kurses zur Sicherheit cyber-physischer Systeme. Die iTrust-Testbeds an der Singapore University of Technology and Design [168], darunter SWaT, WADI und EPIC, sind gut dokumentierte OT-Sicherheitsforschungsumgebungen. Keine dieser Plattformen wurde durch das angewandte Suchprotokoll erfasst, da die entsprechenden Publikationen in Quellen außerhalb der drei durchsuchten Datenbanken erschienen oder primär über institutionelle Repositorien referenziert wurden. Eine gezielte Übersichtsarbeit zu integrierten und domänenspezifischen CR- und TB-Plattformen stellt eine wertvolle Richtung für zukünftige Arbeiten dar.

8. Fazit

Diese Studie untersuchte, wie CRs und Sicherheits-TBs in der Praxis umgesetzt werden, mit Fokus auf die *Technologien*, die zur Realisierung von CR/TB-Szenarien und -Funktionen eingesetzt werden. Aufbauend auf einer systematischen Literaturübersicht über den Zeitraum 2020 bis August 2025 wurden 199 Publikationen umfasst und die extrahierten *Anwendungsbereiche*, *Zwecke*, *Use Cases*, Infrastrukturtypen und berichteten Technologien in einer strukturierten Datengrundlage zur Analyse konsolidiert.

Innerhalb dieser Datengrundlage wurden 650 einzelne Technologien identifiziert und einer hierarchischen Taxonomie mit 10 *Technology Domains* und 81 *Technology Subdomains* zugeordnet, was einen konsistenten Vergleich zwischen den Publikationen trotz heterogener Terminologie und architektonischer Darstellungen ermöglicht. Das Repository erfasst zudem CR/TB-*Zwecke* und *Use Cases* über die *Anwendungsbereiche* hinweg. *Research, Testing and Experimentation* ist der am häufigsten vertretene *Zweck*, und die Literatur deutet auf eine funktionale Trennung in den berichteten Implementierungen hin: TBs werden häufiger für experimentierorientierte *Use Cases* berichtet, während CRs häufiger für *Training and Exercises* und *Education* berichtet werden.

Es ist wichtig anzumerken, dass diese Trennung Muster in *berichteten Implementierungen und Publikationsschwerpunkten* widerspiegelt und keine inhärente technische Einschränkung eines der beiden Plattformtypen darstellt. Wie in Abschnitt 3 angemerkt, können einzelne Publikationen mehrere Zwecke adressieren, und der über CR- und TB-Implementierungen hinweg berichtete Core-Technology-Stack ist im gesamten Korpus weitgehend geteilt (siehe Abschnitt 4.3).

Auf technologischer Ebene ist die *Scenario*-Domäne am häufigsten vertreten, gefolgt von *Red Team Operations* und *Computing Platform*. Mehrere *Anwendungsbereiche* zeigen konzentrierte Profile und explizite Lücken zwischen Domäne und Anwendungsbereich, und die beobachteten zeitlichen Trends deuten auf eine zunehmende Diversifizierung der berichteten *Use Cases* in 2024–2025 hin.

Basierend auf den in der Datengrundlage beobachteten Mustern sowie den diskutierten Herausforderungen einer uneinheitlichen Terminologie und Kategorisierung in der Literatur empfehlen wir, dass zukünftige CR/TB-Publikationen Technologien und Funktionsimplementierungen systematischer berichten (z. B. durch explizite Angabe, welche Komponenten implementiert werden, wie sie integriert sind und welche Tools bestimmte Funktionen operationalisieren). Empfohlen wird weiterhin die Verwendung einer gemeinsamen Terminologie sowie explizite Zuordnungen zu Referenzarchitekturen oder Taxonomien bei der Beschreibung von CR/TB-Fähigkeiten, um Mehrdeutigkeit zu reduzieren und die Vergleichbarkeit zwischen Studien zu verbessern.

Um diese Erkenntnisse für die Praxis nutzbar zu machen, überführt Abschnitt 6 die zentralen Ergebnisse dieser Studie in einen praxisorientierten Leitfaden zur Technologieauswahl für CRs. Dieser Leitfaden fasst die identifizierte Referenzarchitektur, die zugehörigen Feature-Kategorien sowie einen strukturierten, mehrstufigen Auswahlprozess zusammen und richtet sich an Personen und Organisationen, die eine CR konzipieren, beschaffen oder betreiben.

A. Anhang

Die folgende Liste führt alle extrahierten Technologien auf, einschließlich zusätzlicher Informationen zur Kategorisierung, zur Klassifikation als Cyber Range oder Testbed sowie zu den jeweiligen Publikationen. Jede pro Publikation extrahierte Technologie wird einzeln aufgeführt, wodurch mehrere Einträge für dieselbe Technologie entstehen können. Aus Platzgründen wurde die Liste deutlich gekürzt. Bestimmte Details wurden weggelassen, darunter der beabsichtigte Einsatzzweck der Technologie, der Technologietyp (z. B. Tool, Protokoll, Datenformat), feingranulare funktionale Kategorien der Technologie innerhalb der Cyber Range oder des Testbeds, Beschreibungen der *Use Cases* der Technologie, Unterkategorien des *Anwendungsbereichs* der Cyber Range, *Use Cases* der Cyber Range sowie artikelbezogene Informationen. Die Liste enthält die folgenden Spalten:

- **Technologiename** (Technology)
- **Technologiedomäne** (TD)
- **Technologie-Subdomäne** (TSD)
- **Cyber-Range- oder Testbed-Zwecke** (CR/TB P I–III)
- **CR/TB**, gibt an, ob die Publikation eine Cyber Range (CR) oder ein Testbed (TB) beschreibt
- **Quelle**, mit der Referenz zur jeweiligen Publikation
- **Datum**, gibt das Publikationsdatum der Quelle an

Hinweis: Die Spalte **CR/TB P I–III** verwendet folgende Abkürzungen: **Education (E)**, **Research, Testing and Experimentation (RTE)** und **Training and Exercises (TE)**. Ein PDF Export der kompletten Tabelle wurde am Ende des Dokuments angehängt.

Tabelle 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	[157]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2022-12	[157]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2022-12	[157]
Modbus	Scenario	Create/Edit		RTE		TB	2022-12	[157]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2022-12	[157]
PowerWorld	Scenario	Simulation and Emulation		RTE		TB	2022-12	[157]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		TB	2022-12	[157]
Zabbix	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2022-12	[157]
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]
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	[146]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Elastic Logstash	Monitoring and Analytics	Log Management		RTE	TE	CR	2022-06	[146]
Elasticsearch	Data Storage	NoSQL Database		RTE	TE	CR	2022-06	[146]
Esper	Scenario	Infrastructure		RTE	TE	CR	2022-06	[146]
JSON	Scenario	Create/Edit		RTE	TE	CR	2022-06	[146]
Kafka SQL	Scenario	Infrastructure		RTE	TE	CR	2022-06	[146]
Keras	Custom Development	AI & Machine Learning		RTE	TE	CR	2022-06	[146]
MATILDA testbed	Scenario	Create/Edit		RTE	TE	CR	2022-06	[146]
Mouseworld testbed	Scenario	Traffic Generation		RTE	TE	CR	2022-06	[146]
Siddhi	Scenario	Infrastructure		RTE	TE	CR	2022-06	[146]
TensorFlow	Custom Development	AI & Machine Learning		RTE	TE	CR	2022-06	[146]
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 center (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	[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]
AWS Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2024-12	[133]
AWS NoSQL DB	Data Storage	NoSQL Database		RTE		TB	2024-12	[133]
Azure Digital Twins	Computing Platform	Cloud Infrastructure		RTE		TB	2024-12	[133]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-12	[133]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[133]
Google Colab	Custom Development	AI & Machine Learning		RTE		TB	2024-12	[133]

continued on next page

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		TB	2024-12	[133]
MySQL Database	Scenario	Infrastructure		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]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[133]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[133]
Cewl	Red Team Operations	Brute force attacks		RTE		TB	2021-05	[112]
CSV	Custom Development	Dataset Generation		RTE		TB	2021-05	[112]
DVWA	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[112]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2021-05	[112]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-05	[112]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[112]
MQTT	Scenario	Infrastructure		RTE		TB	2021-05	[112]
Nessus	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-05	[112]
Netsniff-ng	Monitoring and Analytics	Data Collection		RTE		TB	2021-05	[112]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-05	[112]
Node-RED	Scenario	Infrastructure		RTE		TB	2021-05	[112]
Ostinato	Scenario	Traffic Generation		RTE		TB	2021-05	[112]
OWASP security Shepherd VM	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[112]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2021-05	[112]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-05	[112]
Vmware NSX	Network Infrastructure	Network Virtualization		RTE		TB	2021-05	[112]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2021-05	[112]
Zeek	Custom Development	Dataset Generation		RTE		TB	2021-05	[112]
DNP3	Scenario	Infrastructure		RTE		TB	2024-01	[123]
EXata network modeling	Network Infrastructure	Network Virtualization		RTE		TB	2024-01	[123]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-01	[123]
RSCAD simulation software	Scenario	Create/Edit		RTE		TB	2024-01	[123]
RTDS simulator	Scenario	Simulation and Emulation		RTE		TB	2024-01	[123]
DNP3	Scenario	Infrastructure		RTE		TB	2024-09	[124]
EXata CPS (Cyber-Physical Network Simulator)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-09	[124]
IEC61850	Scenario	Infrastructure		RTE		TB	2024-09	[124]
IEEE C37.118	Scenario	Infrastructure		RTE		TB	2024-09	[124]
Modbus	Scenario	Create/Edit		RTE		TB	2024-09	[124]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-09	[124]
RTDS simulator	Scenario	Simulation and Emulation		RTE		TB	2024-09	[124]
RT-LAB	Scenario	Simulation and Emulation		RTE		TB	2024-09	[124]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[124]
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	[147]
MongoDB	Data Storage	NoSQL Database		RTE		TB	2025-03	[147]
OCPP	Scenario	Infrastructure		RTE		TB	2025-03	[147]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2025-03	[147]
SQLite	Data Storage	Relational Database		RTE		TB	2025-03	[147]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-03	[147]
Controller Area Network (CAN)	Scenario	Infrastructure		RTE		TB	2022-10	[9]
Avet	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-05	[188]
DVWA	Red Team Operations	Training and Practice Systems		RTE		TB	2021-05	[188]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-05	[188]
Owasp Zap (Zed Attack Proxy)	Red Team Operations	Proxy and Web Interception		RTE		TB	2021-05	[188]
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	[186]
Grafana	Scenario	Infrastructure		RTE		TB	2024-08	[186]
MLFlow	Scenario	Infrastructure		RTE		TB	2024-08	[186]
OBS	Scenario	Infrastructure		RTE		TB	2024-08	[186]
Owncast	Scenario	Infrastructure		RTE		TB	2024-08	[186]
PostgreSQL	Data Storage	Relational Database		RTE		TB	2024-08	[186]
Pynput	Scenario	Infrastructure		RTE		TB	2024-08	[186]
DNP3	Scenario	Infrastructure		RTE	TE	TB	2024-12	[159]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Elasticsearch	Monitoring and Analytics	Log Management		RTE	TE	TB	2024-12	[159]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE	TE	TB	2024-12	[159]
Modbus	Scenario	Infrastructure		RTE	TE	TB	2024-12	[159]
NETLAB+	Portal Services	User Access		RTE	TE	TB	2024-12	[159]
OWASP Juice Shop	Red Team Operations	Training and Practice Systems		RTE	TE	TB	2024-12	[159]
PfSense	Network Infrastructure	Firewall and routing platform		RTE	TE	TB	2024-12	[159]
Security Onion	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[159]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[159]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE	TE	TB	2024-12	[159]
Windows Active Directory	Management	Identity & Access Management (IAM)		RTE	TE	TB	2024-12	[159]
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE	TE	TB	2024-12	[159]
NS2	Network Infrastructure	Network Virtualization		RTE		TB	2022-09	[161]
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]
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	[217]
KITTI Dataset	Scenario	Simulation and Emulation		RTE		TB	2024-11	[217]
GNU Radio	Scenario	Infrastructure		RTE		TB	2025-08	[130]
InfluxDB	Data Storage	Time-series database		RTE		TB	2025-08	[130]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
iPerf3	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-08	[130]
Open5GS	Scenario	Infrastructure		RTE		TB	2025-08	[130]
O-RAN SC	Scenario	Infrastructure		RTE		TB	2025-08	[130]
srsRAN	Scenario	Infrastructure		RTE		TB	2025-08	[130]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2025-08	[130]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-04	[164]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-04	[164]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2022-05	[165]
Asherah NPP Simulator (ANS)	Scenario	Simulation and Emulation		RTE		TB	2024-10	[181]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-10	[181]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-10	[181]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-10	[181]
Modbus	Scenario	Infrastructure		RTE		TB	2024-10	[181]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-10	[181]
Docker	Computing Platform	Containerisation		RTE		TB	2025-06	[101]
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2025-06	[101]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
S7comm	Scenario	Infrastructure		RTE		TB	2025-06	[79]
scapy	Red Team Operations	Paketmanipulation		RTE		TB	2025-06	[79]

continued in Part 02/7

Tabelle 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 center (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	[108]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[108]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[108]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[108]
SSLStrip	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[108]
Tshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-03	[108]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-03	[108]
OpenSSH	Portal Services	Admin Access			TE	CR	2023-08	[150]
OpenStack	Computing Platform	Cloud Infrastructure			TE	CR	2023-08	[150]
proftpd	Scenario	Infrastructure			TE	CR	2023-08	[150]
TightVNC	Scenario	Infrastructure			TE	CR	2023-08	[150]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics			TE	CR	2023-08	[150]
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	[141]
GridLAB-D	Scenario	Simulation and Emulation		RTE		TB	2025-05	[141]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-05	[141]
Modbus	Scenario	Create/Edit		RTE		TB	2025-05	[141]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-05	[141]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2025-05	[141]
GNS3	Network Infrastructure	Network Virtualization		RTE		TB	2022-10	[135]
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	[125]
LAMP stack	Red Team Operations	Training and Practice Systems	E		TE	TB	2025-02	[125]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[151]
Apache web server	Red Team Operations	Training and Practice Systems			TE	CR	2020-08	[151]
DevStack	Computing Platform	Cloud Infrastructure			TE	CR	2020-08	[151]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting			TE	CR	2020-08	[151]
Nmap	Red Team Operations	Network Scanning and Reconnaissance			TE	CR	2020-08	[151]
OpenStack	Computing Platform	Cloud Infrastructure			TE	CR	2020-08	[151]
PyDatalog	Red Team Operations	Attack Strategy & Support			TE	CR	2020-08	[151]
rockyou wordlist	Red Team Operations	Attack Strategy & Support			TE	CR	2020-08	[151]
Wordpress	Red Team Operations	Training and Practice Systems			TE	CR	2020-08	[151]
YAML	Scenario	Create/Edit			TE	CR	2020-08	[151]
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	[136]
Microsoft DoWhy	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[136]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[136]
Scikit-learn	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[136]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[136]
YAWNING-TITAN (YT)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-09	[136]
COPA Zenon SCADA	Scenario	Infrastructure				TB	2021-12	[128]
Dragos OT Asset Visibility and Inventory	Management	Asset & Infrastructure Management				TB	2021-12	[128]
ELK Stack	Monitoring and Analytics	Log Management				TB	2021-12	[128]
GOOSE	Scenario	Infrastructure				TB	2021-12	[128]
Kibana	Monitoring and Analytics	Visualization & Dashboarding				TB	2021-12	[128]
Microsoft Sysmon	Monitoring and Analytics	Log Management				TB	2021-12	[128]
MMS	Scenario	Infrastructure				TB	2021-12	[128]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				TB	2021-12	[128]
Wazuh HIDS	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				TB	2021-12	[128]
Windows Active Directory	Portal Services	Identity & Access Management (IAM)				TB	2021-12	[128]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-10	[102]
CORE	Network Infrastructure	Network Virtualization		RTE		TB	2021-08	[179]
Minimega	Computing Platform	Integrated Cyber Range Solutions		RTE		TB	2021-08	[179]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2021-08	[179]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2021-08	[179]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2021-08	[179]
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	[175]
Elastic Filebeat	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[175]
Elastic Logstash	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[175]
Elasticsearch	Data Storage	Event and Log Storage		RTE		TB	2025-03	[175]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-03	[175]
MITRE ATT&CK	Red Team Operations	Attack Strategy & Support		RTE		TB	2025-03	[175]
MITRE Caldera	Red Team Operations	Adversary emulation		RTE		TB	2025-03	[175]
Winlogbeat	Monitoring and Analytics	Log Management		RTE		TB	2025-03	[175]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-04	[197]
Factory I/O	Scenario	Simulation and Emulation		RTE		TB	2025-04	[197]
Modbus	Scenario	Create/Edit		RTE		TB	2025-04	[197]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-04	[197]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
PfSense	Network Infrastructure	Firewall and routing platform		RTE		TB	2025-04	[197]
ScadaBR	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[197]
UM-NIDS	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[197]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[197]
Ansible	Computing Platform	Software Provisioning and Configuration		RTE		CR	2024-10	[35]
Docker	Computing Platform	Containerisation		RTE		CR	2024-10	[35]
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	[131]
Apache web server	Scenario	Infrastructure		RTE		TB	2025-08	[131]
bpftrace	Scenario	Create/Edit		RTE		TB	2025-08	[131]
eBPF	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-08	[131]
Kubernetes	Computing Platform	Container Orchestration		RTE		TB	2025-08	[131]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2025-08	[131]
libbpf	Scenario	Create/Edit		RTE		TB	2025-08	[131]
Libvirt	Computing Platform	Infrastructure Provisioning and Configuration		RTE		TB	2025-08	[131]
MySQL Database	Data Storage	Relational Database		RTE		TB	2025-08	[131]
Nginx Web server	Scenario	Infrastructure		RTE		TB	2025-08	[131]
Redis database	Data Storage	NoSQL Database		RTE		TB	2025-08	[131]
sysbench	Scenario	Traffic Generation		RTE		TB	2025-08	[131]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-08	[131]
Tomcat web server	Scenario	Infrastructure		RTE		TB	2025-08	[131]
Afra	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-06	[111]
Lingua Franca	Scenario	Create/Edit		RTE		TB	2024-06	[111]
ltsconvert	Scenario	Infrastructure		RTE		TB	2024-06	[111]
Timed Rebeca	Scenario	Simulation and Emulation		RTE		TB	2024-06	[111]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[152]
OPNSense	Network Infrastructure	Firewall and routing platform	E		TE	CR	2023-12	[152]
bwm-ng	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2021-06	[194]
Coin Hive	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[194]
Docker	Computing Platform	Containerisation	E		TE	CR	2021-06	[194]
GENI cloud	Computing Platform	Cloud Infrastructure	E		TE	CR	2021-06	[194]
Geth	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[194]
MariaDB	Data Storage	Relational Database	E		TE	CR	2021-06	[194]
Slowhttptest	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2021-06	[194]
Spring Boot	Custom Development	Backend Frameworks	E		TE	CR	2021-06	[194]
Wireshark	Monitoring and Analytics	Data Collection	E		TE	CR	2021-06	[194]
Ansible	Computing Platform	Software Provisioning and Configuration				CR	2023-12	[127]
Microsoft SQL Database	Data Storage	Relational Database				CR	2023-12	[127]
MySQL Database	Data Storage	Relational Database				CR	2023-12	[127]
SharePoint	Management	Content and Document Management				CR	2023-12	[127]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration				CR	2023-12	[127]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor				CR	2023-12	[127]
Windows Active Directory	Management	Identity & Access Management (IAM)				CR	2023-12	[127]
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]
CURA	Red Team Operations	Training and Practice Systems		RTE		TB	2020-01	[170]
MySQL Database	Data Storage	Relational Database		RTE		TB	2020-01	[170]
OpenPLC	Scenario	Infrastructure		RTE		TB	2020-01	[170]
scapy	Management	Platform & Environment Management		RTE		TB	2020-01	[170]
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	[158]
OpenDSS	Network Infrastructure	Network Virtualization		RTE		TB	2020-04	[158]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[140]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
MQTT	Scenario	Infrastructure		RTE		TB	2025-03	[140]
OpenDSS	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[140]
Typhoon-HIL	Scenario	Simulation and Emulation		RTE		TB	2025-03	[140]
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]

continued in Part 03/7

Tabelle 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	[163]
OpenStack	Computing Platform	Cloud Infrastructure				CR	2021-12	[163]
CarSim	Scenario	Simulation and Emulation		RTE		TB	2024-12	[148]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-12	[148]
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	[118]
DEEP EXPLOIT	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2021-07	[118]
Docker	Computing Platform	Containerisation		RTE		CR	2021-07	[118]
InsightVM	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2021-07	[118]
Metasploitable	Red Team Operations	Training and Practice Systems		RTE		CR	2021-07	[118]
Nikto	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
Nmap	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
OpenVAS	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
Owasp Zap (Zed Attack Proxy)	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
OwaspBWA	Red Team Operations	Training and Practice Systems		RTE		CR	2021-07	[118]
SecGen	Scenario	Create/Edit		RTE		CR	2021-07	[118]
SkipFish	Red Team Operations	Vulnerability Management		RTE		CR	2021-07	[118]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		CR	2021-07	[118]
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2021-07	[118]
Datasets	Custom Development	AI & Machine Learning		RTE		CR	2023-03	[51]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[178]
DeepLog	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[178]
EFK-Stack	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[178]
Free5GC	Scenario	Infrastructure		RTE		TB	2025-02	[178]
h2load	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-02	[178]
Helm	Computing Platform	Container Orchestration		RTE		TB	2025-02	[178]
Istio	Scenario	Create/Edit		RTE		TB	2025-02	[178]
Kubernetes	Computing Platform	Container Orchestration		RTE		TB	2025-02	[178]
LogAnomaly	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[178]
UERANSIM	Scenario	Infrastructure		RTE		TB	2025-02	[178]
Docker	Computing Platform	Containerisation	E	RTE	TE	CR	2021-06	[104]
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	[139]
EVE community edition	Network Infrastructure	Network Virtualization		RTE	TE	CR	2023-04	[139]
Fortinet's log (15-day trial):	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[139]
Fortinet's WAF (15-day trial):	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[139]
Huawei's firewall (30-day trial)	Red Team Operations	Training and Practice Systems		RTE	TE	CR	2023-04	[139]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
VMWare	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE	TE	CR	2023-04	[139]
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]
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]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[115]
eMEGASIM	Scenario	Simulation and Emulation		RTE		TB	2023-12	[115]
EXata network modeling	Network Infrastructure	Network Virtualization		RTE		TB	2023-12	[115]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2023-12	[115]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2023-12	[115]
Python Flask framework	Custom Development	Backend Frameworks		RTE		TB	2023-12	[115]
React.js	Custom Development	Frontend Frameworks		RTE		TB	2023-12	[115]
Factory I/O	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[155]
MATLAB/Simulink	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[155]
Modbus	Scenario	Infrastructure	E		TE	CR	2023-06	[155]
Node-RED	Scenario	Infrastructure	E		TE	CR	2023-06	[155]
OpenPLC	Scenario	Infrastructure	E		TE	CR	2023-06	[155]
PfSense	Network Infrastructure	Firewall and routing platform	E		TE	CR	2023-06	[155]
ScadaBR	Red Team Operations	Training and Practice Systems	E		TE	CR	2023-06	[155]
Unity3D	Scenario	Simulation and Emulation	E		TE	CR	2023-06	[155]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor	E		TE	CR	2023-06	[155]
Modbus	Scenario	Create/Edit		RTE		TB	2024-10	[171]
NS3	Network Infrastructure	Network Virtualization		RTE		TB	2024-10	[171]
RTDS	Scenario	Simulation and Emulation		RTE		TB	2024-10	[171]
LightGBM	Custom Development	AI & Machine Learning		RTE		CR	2022-08	[218]
Modbus	Scenario	Infrastructure		RTE		CR	2022-08	[218]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
OPC Unified Architecture (OPC-UA)	Scenario	Infrastructure		RTE		CR	2022-08	[218]
Unity3D	Scenario	Simulation and Emulation		RTE		CR	2022-08	[218]
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]
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	[121]
Docker	Computing Platform	Containerisation	E		TE	CR	2024-03	[121]
Gdb	Custom Development	Debugger	E		TE	CR	2024-03	[121]
Gef	Custom Development	Debugger	E		TE	CR	2024-03	[121]
Ghidra	Blue Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2024-03	[121]
Ipython	Custom Development	Integrated Development Environment	E		TE	CR	2024-03	[121]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	E		TE	CR	2024-03	[121]
OpenSSH	Portal Services	User Access	E		TE	CR	2024-03	[121]
Pwndbg	Red Team Operations	Attack Strategy & Support	E		TE	CR	2024-03	[121]
Pwntools	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2024-03	[121]
QEMU	Computing Platform	Virtualization platform/Type-2-Hypervisor	E		TE	CR	2024-03	[121]
Radare2	Blue Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2024-03	[121]
scapy	Red Team Operations	Paketmanipulation	E		TE	CR	2024-03	[121]
SLIRP	Scenario	Infrastructure	E		TE	CR	2024-03	[121]
Strace	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2024-03	[121]
Tmux	Portal Services	User Access	E		TE	CR	2024-03	[121]
VS Code	Portal Services	User Access	E		TE	CR	2024-03	[121]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E		TE	CR	2024-03	[121]
HYPERSIM	Scenario	Simulation and Emulation		RTE		TB	2024-01	[156]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-01	[156]
OpalTarget OP5707XG	Scenario	Simulation and Emulation		RTE		TB	2024-01	[156]
Open Charge Point Protocol (OCPP)	Scenario	Infrastructure		RTE		TB	2024-01	[156]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
VMWare vSphere	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-01	[156]
aircrack-ng	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[134]
Airgeddon	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[134]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2024-12	[134]
Arduino IDE	Custom Development	Integrated Development Environment		RTE		TB	2024-12	[134]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-12	[134]
Ettercap	Red Team Operations	Paketmanipulation		RTE		TB	2024-12	[134]
Flower Framework	Custom Development	AI & Machine Learning		RTE		TB	2024-12	[134]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2024-12	[134]
Hping	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[134]
MySQL Database	Data Storage	Relational Database		RTE		TB	2024-12	[134]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[134]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2024-12	[134]
Tracemalloc	Scenario	Infrastructure		RTE		TB	2024-12	[134]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-12	[134]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-12	[134]
DNP3	Scenario	Infrastructure			TE	TB	2020-10	[144]
GOOSE	Scenario	Infrastructure			TE	TB	2020-10	[144]

continued in Part 04/7

Tabelle 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	[144]
Opal-RT Simulator	Scenario	Simulation and Emulation			TE	TB	2020-10	[144]
OpenPDC	Scenario	Simulation and Emulation			TE	TB	2020-10	[144]
RT-LAB	Scenario	Simulation and Emulation			TE	TB	2020-10	[144]
SIEMENS SICAM PAS	Scenario	Infrastructure			TE	TB	2020-10	[144]
VMWare	Computing Platform	Virtualization platform/Type-2-Hypervisor			TE	TB	2020-10	[144]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-12	[183]
Memtester	Scenario	Infrastructure		RTE		TB	2024-12	[183]
Mosquitto MQTT Broker	Red Team Operations	Training and Practice Systems		RTE		TB	2024-12	[183]
MQTT benchmarking tool	Scenario	Infrastructure		RTE		TB	2024-12	[183]
5g-trace-visualizer	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[201]
CSV	Custom Development	Dataset Generation		RTE		TB	2024-09	[201]
Free5GC	Scenario	Infrastructure		RTE		TB	2024-09	[201]
free5gc-compose	Scenario	Create/Edit		RTE		TB	2024-09	[201]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2024-09	[201]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[201]
Transformers	Custom Development	AI & Machine Learning		RTE		TB	2024-09	[201]
Tshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[201]
UERANSIM	Scenario	Infrastructure		RTE		TB	2024-09	[201]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2024-09	[201]
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]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[193]
CTFd	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[193]
Docker	Computing Platform	Containerisation	E		TE	CR	2024-05	[193]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service	E		TE	CR	2024-05	[193]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2024-05	[193]
MySQL Database	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[193]
Naumachia	Computing Platform	Infrastructure Instantiation Systems	E		TE	CR	2024-05	[193]
OpenSSH	Portal Services	User Access	E		TE	CR	2024-05	[193]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E		TE	CR	2024-05	[193]
Sqlmap	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2024-05	[193]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance	E		TE	CR	2024-05	[193]
Wordpress	Red Team Operations	Training and Practice Systems	E		TE	CR	2024-05	[193]
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]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
SV	Scenario	Infrastructure		RTE		TB	2024-08	[105]
Docker	Computing Platform	Containerisation		RTE		TB	2024-09	[184]
httperf	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-09	[184]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		TB	2024-09	[184]
Memtester	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2024-09	[184]
simpy	Scenario	Infrastructure		RTE		TB	2024-09	[184]
TeaStore	Red Team Operations	Training and Practice Systems		RTE		TB	2024-09	[184]
TimeNET	Scenario	Infrastructure		RTE		TB	2024-09	[184]
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]
airmon-ng	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[116]
EXata CPS (Cyber-Physical Network Simulator)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-04	[116]
hcitool scan	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[116]
Medusa	Red Team Operations	Brute force attacks		RTE		TB	2024-04	[116]
MobSF (Mobile Security Framework)	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2024-04	[116]
Netdiscover	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-04	[116]
Nikto	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[116]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-04	[116]
OpenVAS	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[116]
Owasp Zap (Zed Attack Proxy)	Blue Team Operations	Vulnerability Management		RTE		TB	2024-04	[116]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-10	[215]
Modbus	Scenario	Infrastructure		RTE		TB	2024-10	[215]
MySQL Database	Data Storage	Relational Database		RTE		TB	2024-10	[215]
OpenWrt	Scenario	Infrastructure		RTE		TB	2024-10	[215]
pySCADA	Scenario	Simulation and Emulation		RTE		TB	2024-10	[215]
rapidSCADA	Scenario	Simulation and Emulation		RTE		TB	2024-10	[215]
rsyslog	Monitoring and Analytics	Log Management		RTE		TB	2024-10	[215]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2024-10	[215]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2024-10	[215]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-10	[215]
Gazebo	Scenario	Simulation and Emulation		RTE		TB	2025-03	[191]
MAVLink	Scenario	Infrastructure		RTE		TB	2025-03	[191]
PX4 Autopilot	Scenario	Simulation and Emulation		RTE		TB	2025-03	[191]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
ROS (Robot Operating System)	Scenario	Simulation and Emulation		RTE		TB	2025-03	[191]
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]
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	[167]
BUP Benign User Profiler	Scenario	Traffic Generation		RTE		CR	2025-02	[167]
CSV	Custom Development	Dataset Generation		RTE		CR	2025-02	[167]
HERA	Custom Development	Dataset Generation		RTE		CR	2025-02	[167]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		CR	2025-02	[167]
HULK	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		CR	2025-02	[167]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		CR	2025-02	[167]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2025-02	[167]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-02	[167]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
PCAPNG	Custom Development	Dataset Generation		RTE		CR	2025-02	[167]
SecLists Password Dictionary	Red Team Operations	Attack Strategy & Support		RTE		CR	2025-02	[167]
Wireshark	Monitoring and Analytics	Data Collection		RTE		CR	2025-02	[167]
Cisco Cyber Vision	Monitoring and Analytics	Analysis & Verification			TE	TB	2021-08	[137]
Factory I/O	Scenario	Simulation and Emulation			TE	TB	2021-08	[137]
Home I/O	Scenario	Simulation and Emulation			TE	TB	2021-08	[137]
Microsoft Threat Modeling Tool	Red Team Operations	Attack Strategy & Support			TE	TB	2021-08	[137]
Modbus	Scenario	Infrastructure			TE	TB	2021-08	[137]
Nginx Web server	Red Team Operations	Attack Strategy & Support			TE	TB	2021-08	[137]
Rubber Ducky	Red Team Operations	Exploitation and Attack Execution			TE	TB	2021-08	[137]
simpy	Scenario	Infrastructure			TE	TB	2021-08	[137]
Windows Remote desktop protocol (RDP)	Red Team Operations	Attack Strategy & Support	E		TE	TB	2021-08	[137]
EXata network modeling	Network Infrastructure	Network Virtualization		RTE		TB	2025-03	[176]
HYPERSIM	Scenario	Simulation and Emulation		RTE		TB	2025-03	[176]
Modbus	Scenario	Infrastructure		RTE		TB	2025-03	[176]
CARLA	Scenario	Simulation and Emulation		RTE		TB	2025-06	[172]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2025-06	[172]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2025-06	[172]
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]
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	[162]
QEMU-IOL	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		CR	2021-01	[162]
Step7-MicroWin	Custom Development	Integrated Development Environment		RTE		CR	2021-01	[162]
WinSCP	Management	Platform & Environment Management		RTE		CR	2021-01	[162]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[110]
Cewl	Red Team Operations	Brute force attacks		RTE		TB	2025-03	[110]
Ettercap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[110]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[110]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2025-03	[110]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[110]
Mosquitto MQTT Broker	Red Team Operations	Training and Practice Systems		RTE		TB	2025-03	[110]
MySQL Workbench	Custom Development	Dataset Generation		RTE		TB	2025-03	[110]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[110]
Node-RED	Custom Development	Integrated Development Environment		RTE		TB	2025-03	[110]
SAir-IIoT Cyber Testbed	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-03	[110]
scapy	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[110]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[110]
UFONet	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-03	[110]
VMWare Workstation	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2025-03	[110]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-03	[110]
Xprobe2	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-03	[110]
Xsser	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2025-03	[110]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure				CR	2021-11	[180]
Packer	Computing Platform	Infrastructure Provisioning and Configuration				CR	2021-11	[180]
Terraform	Computing Platform	Infrastructure Provisioning and Configuration				CR	2021-11	[180]
YAML	Management	Asset & Infrastructure Management				CR	2021-11	[180]
CTFd	Red Team Operations	Training and Practice Systems	E	RTE	TE	CR	2025-01	[219]
OpenStack	Computing Platform	Cloud Infrastructure	E	RTE	TE	CR	2025-01	[219]
Prometheus	Monitoring and Analytics	Assets Monitoring	E	RTE	TE	CR	2025-01	[219]

continued in Part 05/7

Tabelle 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]
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]

continued on next page

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	2023-07	[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	[214]
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	[154]
DNP3	Scenario	Infrastructure		RTE		TB	2024-10	[154]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-10	[154]
Matrikon OPC	Scenario	Infrastructure		RTE		TB	2024-10	[154]
Triangle Microworks DTM	Scenario	Infrastructure		RTE		TB	2024-10	[154]
Burp	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2022-05	[207]
CTFd	Red Team Operations	Training and Practice Systems	E		TE	CR	2022-05	[207]
Datalog	Custom Development	Programming language	E		TE	CR	2022-05	[207]
Hydra	Red Team Operations	Password Cracking and Credential Harvesting	E		TE	CR	2022-05	[207]
Immunity Debugger	Red Team Operations	Reverse Engineering and Binary Analysis	E		TE	CR	2022-05	[207]
JSON	Scenario	Create/Edit	E		TE	CR	2022-05	[207]
Metasploit	Red Team Operations	Exploitation and Attack Execution	E		TE	CR	2022-05	[207]
Nmap	Red Team Operations	Network Scanning and Reconnaissance	E		TE	CR	2022-05	[207]
OpenStack	Computing Platform	Cloud Infrastructure	E		TE	CR	2022-05	[207]
Wireshark	Monitoring and Analytics	Analysis & Verification	E		TE	CR	2022-05	[207]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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	[199]
NIST Randomness Test Suite	Blue Team Operations	Vulnerability Management		RTE		TB	2025-02	[199]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[199]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2024-03	[109]
Opal-RT Simulator	Scenario	Simulation and Emulation		RTE		TB	2024-03	[109]
OpenPDC	Scenario	Infrastructure		RTE		TB	2024-03	[109]
scapy	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[109]
Tcpdump	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[109]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-03	[109]
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	[206]
NMEA 0183	Scenario	Infrastructure		RTE		TB	2022-08	[206]
OpenCPN	Scenario	Simulation and Emulation		RTE		TB	2022-08	[206]
scapy	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2022-08	[206]
DNP3	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
GE eTerra PhasorPoint	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
GOOSE	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
MMS	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
Opal-RT Simulator	Scenario	Simulation and Emulation	E	RTE	TE	TB	2020-10	[145]
OpenPDC	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
PfSense	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
SIEMENS SICAM PAS	Scenario	Infrastructure	E	RTE	TE	TB	2020-10	[145]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E	RTE	TE	TB	2020-10	[145]
Suricata	Blue Team Operations	Firewalls & Network Security Gateways	E	RTE	TE	TB	2020-10	[145]
untangle	Blue Team Operations	Firewalls & Network Security Gateways	E	RTE	TE	TB	2020-10	[145]
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)	E	RTE	TE	TB	2020-10	[145]
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	[202]
CyberVAN	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-02	[202]
Elastic Beats	Monitoring and Analytics	Log Management		RTE		TB	2025-02	[202]
MySQL Database	Red Team Operations	Training and Practice Systems		RTE		TB	2025-02	[202]
Security Onion	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2025-02	[202]
MATLAB/Simulink	Scenario	Infrastructure				TB	2023-12	[149]
MongoDB	Scenario	Infrastructure				TB	2023-12	[149]
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	[114]
CSV	Scenario	Infrastructure		RTE		TB	2024-12	[114]
Docker	Computing Platform	Containerisation		RTE		TB	2024-12	[114]
InfluxDB	Data Storage	Time-series database		RTE		TB	2024-12	[114]
iPerf	Monitoring and Analytics	Analysis & Verification		RTE		TB	2024-12	[114]
Keysight Open RAN Architect (KORA)	Scenario	Infrastructure		RTE		TB	2024-12	[114]
Kubernetes	Scenario	Infrastructure		RTE		TB	2024-12	[114]
Matlabs 4G toolbox	Scenario	Infrastructure		RTE		TB	2024-12	[114]
Matlabs 5G toolbox	Scenario	Infrastructure		RTE		TB	2024-12	[114]
MAVLink	Scenario	Infrastructure		RTE		TB	2024-12	[114]
NSF POWDER Wireless platform	Computing Platform	Integrated Testbed Solutions		RTE		TB	2024-12	[114]
srsRAN	Scenario	Infrastructure		RTE		TB	2024-12	[114]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2024-12	[114]
CVSS	Blue Team Operations	Vulnerability Management		RTE		CR	2024-09	[80]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Microsoft CyberBattleSim	Computing Platform	Integrated Testbed Solutions		RTE		CR	2024-09	[80]
PfSense	Scenario	Infrastructure		RTE		CR	2024-07	[196]
Skytap	Computing Platform	Cloud Infrastructure		RTE		CR	2024-07	[196]
Splunk	Blue Team Operations	SIEM & Security Analytics		RTE		CR	2024-07	[196]
Windows Task Scheduler	Scenario	Simulation and Emulation		RTE		CR	2024-07	[196]
Wordpress	Management	Content and Document Management		RTE		CR	2024-07	[196]
XAMPP	Scenario	Infrastructure		RTE		CR	2024-07	[196]
gym-pybullet-drones	Scenario	Simulation and Emulation		RTE		TB	2024-11	[198]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-11	[198]
Optuna	Custom Development	AI & Machine Learning		RTE		TB	2024-11	[198]
PyBullet Physics Engine	Scenario	Simulation and Emulation		RTE		TB	2024-11	[198]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2024-11	[198]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2024-11	[198]
Apache web server	Red Team Operations	Training and Practice Systems		RTE		TB	2025-05	[143]
Aposemat IoT-23 Dataset	Scenario	Infrastructure		RTE		TB	2025-05	[143]
CICIOT-2023	Scenario	Infrastructure		RTE		TB	2025-05	[143]
CSV	Custom Development	Dataset Generation		RTE		TB	2025-05	[143]
DPKT	Custom Development	Dataset Generation		RTE		TB	2025-05	[143]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-05	[143]
P4 BMv2 software switch	Scenario	Infrastructure		RTE		TB	2025-05	[143]
P4Utils	Scenario	Infrastructure		RTE		TB	2025-05	[143]
Pandas	Custom Development	Dataset Generation		RTE		TB	2025-05	[143]
scapy	Monitoring and Analytics	Data Collection		RTE		TB	2025-05	[143]
Slowloris	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-05	[143]
Tcpreplay	Monitoring and Analytics	Data Collection		RTE		TB	2025-05	[143]
CyRIS	Computing Platform	Infrastructure Instantiation Systems		RTE		CR	2025-01	[122]
Iptables/nftables	Network Infrastructure	Firewall and routing platform		RTE		CR	2025-01	[122]
KVM	Computing Platform	Virtualization platform/Type-1-Hypervisor		RTE		CR	2025-01	[122]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2025-01	[122]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-01	[122]
pymetasploit3	Red Team Operations	Attack Strategy & Support		RTE		CR	2025-01	[122]
python-nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2025-01	[122]
YAML	Scenario	Create/Edit		RTE		CR	2025-01	[122]
Apache JMeter	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[160]
cpprestsdk	Custom Development	Simulation Environment		RTE		TB	2025-04	[160]
Docker	Computing Platform	Containerisation		RTE		TB	2025-04	[160]
Hyperledger Composer	Scenario	Infrastructure		RTE		TB	2025-04	[160]
Hyperledger Fabric	Scenario	Infrastructure		RTE		TB	2025-04	[160]
Node.js	Custom Development	Backend Frameworks		RTE		TB	2025-04	[160]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
ProVerif	Monitoring and Analytics	Analysis & Verification		RTE		TB	2025-04	[160]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2025-04	[160]
VENTOS	Scenario	Simulation and Emulation		RTE		TB	2025-04	[160]
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	[203]
MQTT	Scenario	Infrastructure		RTE		TB	2025-01	[203]
OpenTAP	Scenario	Controlling		RTE		TB	2025-01	[203]
PASTA (Portable Automotive Security Testbed with Adaptability)	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-01	[203]
Unity3D	Scenario	Simulation and Emulation		RTE		TB	2025-01	[203]

continued in Part 06/7

Tabelle 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	[200]
OPNET	Network Infrastructure	Network Virtualization		RTE		TB	2021-04	[200]
RT-LAB	Scenario	Simulation and Emulation		RTE		TB	2021-04	[200]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure		RTE		TB	2021-12	[166]
JSON	Scenario	Infrastructure		RTE		TB	2021-12	[166]
MATLAB/Simulink	Scenario	Simulation and Emulation		RTE		TB	2021-12	[166]
Modbus	Scenario	Infrastructure		RTE		TB	2021-12	[166]
MQTT	Scenario	Infrastructure		RTE		TB	2021-12	[166]
Node-RED	Custom Development	Integrated Development Environment		RTE		TB	2021-12	[166]
DNP3	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[174]
GRFICS	Scenario	Simulation and Emulation	E	RTE	TE	TB	2024-12	[174]
Ignition SCADA	Custom Development	Visualization & Dashboarding	E	RTE	TE	TB	2024-12	[174]
Modbus	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[174]
NETLAB+	Portal Services	User Access	E	RTE	TE	TB	2024-12	[174]
OPC Unified Architecture (OPC-UA)	Custom Development	Visualization & Dashboarding	E	RTE	TE	TB	2024-12	[174]
OpenPLC	Scenario	Infrastructure	E	RTE	TE	TB	2024-12	[174]
Typhoon-HIL	Scenario	Simulation and Emulation	E	RTE	TE	TB	2024-12	[174]
VMWare ESXi	Computing Platform	Virtualization platform/Type-1-Hypervisor	E	RTE	TE	TB	2024-12	[174]
ANSYS	Scenario	Infrastructure		RTE		TB	2020-06	[211]
MATLAB/Simulink	Scenario	Infrastructure		RTE		TB	2020-06	[211]
Opal-RT Simulator	Scenario	Infrastructure		RTE		TB	2020-06	[211]
Docker	Computing Platform	Containerisation		RTE		CR	2025-03	[216]
Node.js	Scenario	Create/Edit		RTE		CR	2025-03	[216]
Npm	Scenario	Create/Edit		RTE		CR	2025-03	[216]
OSV Open Source Vulnerability	Scenario	Create/Edit		RTE		CR	2025-03	[216]
PyPI		Create/Edit		RTE		CR	2025-03	[216]
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]
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	[189]
Elastic Auditbeat	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[189]
Elastic Logstash	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[189]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Elasticsearch	Monitoring and Analytics	Log Management		RTE		TB	2021-12	[189]
Kibana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2021-12	[189]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-12	[189]
Microsoft Sysmon	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[189]
Mimikatz	Red Team Operations	Password Cracking and Credential Harvesting		RTE		TB	2021-12	[189]
Packer	Computing Platform	Infrastructure Provisioning and Configuration		RTE		TB	2021-12	[189]
Packetbeat	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[189]
Reg	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-12	[189]
Selenium	Scenario	User Behavior Simulation		RTE		TB	2021-12	[189]
Sigma	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2021-12	[189]
Sqlmap	Red Team Operations	Exploitation and Attack Execution		RTE		TB	2021-12	[189]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2021-12	[189]
Tcpreplay	Monitoring and Analytics	Data Collection		RTE		TB	2021-12	[189]
VirtualBox	Computing Platform	Virtualization platform/Type-2-Hypervisor		RTE		TB	2021-12	[189]
Xcopy	Red Team Operations	Attack Strategy & Support		RTE		TB	2021-12	[189]
BB84	Scenario	Infrastructure		RTE		TB	2024-09	[138]
MATLAB	Scenario	Infrastructure		RTE		TB	2024-09	[138]
NS3	Scenario	Simulation and Emulation		RTE		TB	2024-09	[138]
OpenVirteX	Scenario	Infrastructure		RTE		TB	2024-09	[138]
QKDNetSim	Scenario	Simulation and Emulation		RTE		TB	2024-09	[138]
Ryu	Scenario	Infrastructure		RTE		TB	2024-09	[138]
TapBridge	Scenario	Infrastructure		RTE		TB	2024-09	[138]
DNP3	Scenario	Infrastructure		RTE		TB	2021-10	[117]
MATPOWER	Scenario	Simulation and Emulation		RTE		TB	2021-10	[117]
NS3	Scenario	Infrastructure		RTE		TB	2021-10	[117]
PingThings Berkeley Tree Database (BTrDB)	Data Storage	Time-series database		RTE		TB	2021-10	[117]
PSSE	Scenario	Simulation and Emulation		RTE		TB	2021-10	[117]
RTDS	Scenario	Simulation and Emulation		RTE		TB	2021-10	[117]
Splunk	Monitoring and Analytics	Log Management		RTE		TB	2021-10	[117]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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]
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	[185]
Iptables/nftables	Scenario	Infrastructure		RTE		TB	2025-08	[185]
Modbus	Scenario	Infrastructure		RTE		TB	2025-08	[185]
OpenPLC	Scenario	Infrastructure		RTE		TB	2025-08	[185]
PyCryptodome	Scenario	Create/Edit		RTE		TB	2025-08	[185]
pyModbus	Scenario	Infrastructure		RTE		TB	2025-08	[185]
scapy	Scenario	Infrastructure		RTE		TB	2025-08	[185]
tc netem	Scenario	Infrastructure		RTE		TB	2025-08	[185]
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	[132]
Binary Ninja	Custom Development	Reverse Engineering and Binary Analysis		RTE		TB	2020-05	[132]
CARLA	Scenario	Simulation and Emulation		RTE		TB	2020-05	[132]
CUDA	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[132]
Mambo	Scenario	Infrastructure		RTE		TB	2020-05	[132]
Mcsema	Scenario	Infrastructure		RTE		TB	2020-05	[132]
SVF library	Scenario	Infrastructure		RTE		TB	2020-05	[132]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[132]
Tensorflow Lite	Custom Development	AI & Machine Learning		RTE		TB	2020-05	[132]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
ZeroMQ	Scenario	Infrastructure		RTE		TB	2020-05	[132]
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]
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	[113]
MANO	Scenario	Infrastructure		RTE		TB	2020-04	[113]
ONOS	Scenario	Infrastructure		RTE		TB	2020-04	[113]
OpenFlow	Scenario	Infrastructure		RTE		TB	2020-04	[113]
OpenStack	Computing Platform	Cloud Infrastructure		RTE		TB	2020-04	[113]
scapy	Red Team Operations	Paketmanipulation		RTE		TB	2020-04	[113]
sFlow	Monitoring and Analytics	Analysis & Verification		RTE		TB	2020-04	[113]
URLhaus	Blue Team Operations	Malware Analysis		RTE		TB	2020-04	[113]
YAML	Scenario	Infrastructure		RTE		TB	2020-04	[113]
Zeek	Monitoring and Analytics	Analysis & Verification		RTE		TB	2020-04	[113]
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]
Vulnerability Reproduction Tool (VRT)	Scenario	Infrastructure		RTE		TB	2025-01	[29]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Zeek	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-01	[29]
curl-loader	Scenario	Traffic Generation		RTE		TB	2025-02	[142]
Hping	Red Team Operations	Denial of Service & Distributed Denial of Service		RTE		TB	2025-02	[142]
Keras	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[142]
Matplotlib	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2025-02	[142]
Mininet	Network Infrastructure	Network Virtualization		RTE		TB	2025-02	[142]
NetworkX	Scenario	Infrastructure		RTE		TB	2025-02	[142]
NumPy	Custom Development	Data Science		RTE		TB	2025-02	[142]
OpenFlow	Scenario	Infrastructure		RTE		TB	2025-02	[142]
Pandas	Custom Development	Data Science		RTE		TB	2025-02	[142]
Ryu	Scenario	Infrastructure		RTE		TB	2025-02	[142]
Seaborn	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[142]
Tcpdump	Monitoring and Analytics	Data Collection		RTE		TB	2025-02	[142]
TensorFlow	Custom Development	AI & Machine Learning		RTE		TB	2025-02	[142]
Tshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-02	[142]
MITRE ATT&CK	Blue Team Operations	Threat Intelligence		RTE		TB	2025-01	[153]
MITRE Caldera	Red Team Operations	Adversary emulation		RTE		TB	2025-01	[153]
MulVAL	Red Team Operations	Network Scanning and Reconnaissance		RTE		TB	2025-01	[153]
Suricata	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)		RTE		TB	2025-01	[153]
Wazuh SIEM	Blue Team Operations	SIEM & Security Analytics		RTE		TB	2025-01	[153]
Windows Active Directory	Portal Services	Identity & Access Management (IAM)		RTE		TB	2025-01	[153]
IEC 60870-5-104	Scenario	Infrastructure		RTE		TB	2025-06	[195]
IPAL Toolset	Custom Development	Dataset Generation		RTE		TB	2025-06	[195]
PowerOwl	Scenario	Simulation and Emulation		RTE		TB	2025-06	[195]
Simbench	Scenario	Infrastructure		RTE		TB	2025-06	[195]
Wattson	Computing Platform	Integrated Testbed Solutions		RTE		TB	2025-06	[195]
Cyber Physical Systems Wind Tunnel (CPSWT)	Scenario	Simulation and Emulation		RTE		TB	2020-09	[120]
Grafana	Monitoring and Analytics	Visualization & Dashboarding		RTE		TB	2020-09	[120]
InfluxDB	Data Storage	Time-series database		RTE		TB	2020-09	[120]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2020-09	[120]
SocketCAN	Scenario	Infrastructure		RTE		TB	2020-09	[120]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2020-09	[120]
V2X	Scenario	Simulation and Emulation		RTE		TB	2020-09	[120]
Veins	Scenario	Simulation and Emulation		RTE		TB	2020-09	[120]
WebGME	Scenario	Controlling		RTE		TB	2020-09	[120]
ZeroMQ	Scenario	Infrastructure		RTE		TB	2020-09	[120]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Anaconda	Custom Development	AI & Machine Learning		RTE		TB	2025-04	[192]
Apache Spark	Custom Development	AI & Machine Learning		RTE		TB	2025-04	[192]
CICFlowMeter	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[192]
CSV	Scenario	Infrastructure		RTE		TB	2025-04	[192]
Jupyter notebook	Custom Development	Integrated Development Environment		RTE		TB	2025-04	[192]
NumPy	Custom Development	Data Science		RTE		TB	2025-04	[192]
Wireshark	Monitoring and Analytics	Data Collection		RTE		TB	2025-04	[192]
XAMPP	Scenario	Infrastructure		RTE		TB	2025-04	[192]
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	[126]
Docker Hub	Computing Platform	Infrastructure Provisioning and Configuration	E		TE	CR	2020-10	[126]
Docker Swarm	Computing Platform	Container Orchestration	E		TE	CR	2020-10	[126]
DVWA	Red Team Operations	Training and Practice Systems	E		TE	CR	2020-10	[126]
Amazon Web Services (AWS)	Computing Platform	Cloud Infrastructure	E		TE	CR	2024-09	[64]

continued in Part 07/7

Tabelle 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]
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]

continued on next page

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	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	[177]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2022-03	[177]
PsTools	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-03	[177]
Wireshark	Blue Team Operations	Network Analysis & Reconnaissance		RTE	TE	TB	2022-03	[177]
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]
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]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
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]
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	[208]
CSV	Scenario	Infrastructure		RTE		CR	2022-09	[208]
Datalog	Custom Development	Programming language		RTE		CR	2022-09	[208]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2022-09	[208]
Mimikatz	Red Team Operations	Exploitation and Attack Execution		RTE		CR	2022-09	[208]
nbtscan	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[208]
Netdiscover	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[208]
Nmap	Red Team Operations	Network Scanning and Reconnaissance		RTE		CR	2022-09	[208]
Norwegian Cyber Range	Computing Platform	Integrated Cyber Range Solutions		RTE		CR	2022-09	[208]
PyDatalog	Red Team Operations	Attack Strategy & Support		RTE		CR	2022-09	[208]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
VNCDtool	Scenario	Traffic Generation		RTE		CR	2022-09	[208]
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]
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	[182]
Nmap	Red Team Operations	Network Scanning and Reconnaissance				CR	2022-08	[182]
SCORCH	Scenario	Controlling				CR	2022-08	[182]
Snort	Blue Team Operations	Intrusion Detection & Prevention (IDS/IPS)				CR	2022-08	[182]
INET	Scenario	Create/Edit		RTE		TB	2024-01	[173]
OMNeT++	Scenario	Simulation and Emulation		RTE		TB	2024-01	[173]
Scyther	Blue Team Operations	Vulnerability Management		RTE		TB	2024-01	[173]
SUMO	Scenario	Simulation and Emulation		RTE		TB	2024-01	[173]
Tamarin Prover	Scenario	Infrastructure		RTE		TB	2024-01	[173]
Veins	Scenario	Simulation and Emulation		RTE		TB	2024-01	[173]
Android Emulator	Scenario	Simulation and Emulation		RTE	TE	TB	2022-08	[205]
asn1c tool	Custom Development	Build-Toolchain		RTE	TE	TB	2022-08	[205]
Bettercap	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-08	[205]
Docker	Computing Platform	Containerisation		RTE	TE	TB	2022-08	[205]
Hydra	Red Team Operations	Brute force attacks		RTE	TE	TB	2022-08	[205]
JupyterHub	Portal Services	User Access		RTE	TE	TB	2022-08	[205]
Kubernetes	Computing Platform	Infrastructure Provisioning and Configuration		RTE	TE	TB	2022-08	[205]
Metasploit	Red Team Operations	Exploitation and Attack Execution		RTE	TE	TB	2022-08	[205]
MongoDB	Data Storage	NoSQL Database		RTE	TE	TB	2022-08	[205]
OAIs gNB emulator	Scenario	Infrastructure		RTE	TE	TB	2022-08	[205]
OAuth 2.0	Portal Services	Identity & Access Management (IAM)		RTE	TE	TB	2022-08	[205]
Openapi-generator	Scenario	Infrastructure		RTE	TE	TB	2022-08	[205]
P4 BMv2 software switch	Scenario	Infrastructure		RTE	TE	TB	2022-08	[205]
sFuzz	Red Team Operations	Vulnerability Management		RTE	TE	TB	2022-08	[205]
Tcpdump	Monitoring and Analytics	Data Collection		RTE	TE	TB	2022-08	[205]
wfuzz	Red Team Operations	Vulnerability Management		RTE	TE	TB	2022-08	[205]
Wireshark	Red Team Operations	Network Scanning and Reconnaissance		RTE	TE	TB	2022-08	[205]

continued on next page

Technology	TD	TSD	CR/TB P I	CR/TB P II	CR/TB P III	CR/TB	Date	Source
Controller Area Network (CAN)	Scenario	Infrastructure		RTE		TB	2023-07	[212]
LIN	Scenario	Infrastructure		RTE		TB	2023-07	[212]
SavvyCan	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[212]
scapy	Red Team Operations	Vulnerability Management		RTE		TB	2023-07	[212]
TSMaster	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[212]
VXDIAG VCX Professional Car Diagnostic	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[212]
Wireshark	Monitoring and Analytics	Analysis & Verification		RTE		TB	2023-07	[212]
Docker	Computing Platform	Containerisation		RTE		TB	2025-06	[187]
Helm	Computing Platform	Container Orchestration		RTE		TB	2025-06	[187]
Kubernetes	Scenario	Infrastructure		RTE		TB	2025-06	[187]
MITRE CAPEC	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[187]
MITRE CWE	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[187]
NumPy	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[187]
NVD	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[187]
O-RAN SC	Scenario	Infrastructure		RTE		TB	2025-06	[187]
Pandas	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[187]
PyTorch	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[187]
Transformers	Custom Development	AI & Machine Learning		RTE		TB	2025-06	[187]
Trivy	Blue Team Operations	Vulnerability Management		RTE		TB	2025-06	[187]
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]

Literatur

[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). DOI 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). DOI 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). DOI 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 Reports **12**, 1655–1672 (2024). DOI 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. Computer Networks **247**, 110446 (2024). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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 - International Journal of Electronics and Communications **171**, 154913 (2023). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. International Journal of Critical Infrastructure Protection **42**, 100618 (2023). DOI 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). DOI 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). DOI 10.1016/j.cose.2023.103201

[28] Busquim e 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Progress in Nuclear Energy **175**, 105348 (2024). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Applied Sciences **11**(4), 1809 (2021). DOI 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). DOI 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). DOI 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. Applied Sciences **11**(20), 9509 (2021). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Computers in Industry **148**, 103906 (2023). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Computers and Electrical Engineering **126**, 110543 (2025). DOI 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). DOI 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. Journal of Network and Computer Applications **229**, 103918 (2024). DOI 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). URL `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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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 in Brief **57**, 111153 (2024). DOI 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). DOI 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 Transactions on Industrial Electronics **67**(3), 2371–2379 (2020). DOI 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). DOI 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 Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS '22, pp. 9–16. Association for Computing Machinery, New York, NY, USA (2022). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Computers and Electrical Engineering **101**, 108061 (2022). DOI 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). DOI 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. International Journal of Information Security **22**(4), 1005–1027 (2023). DOI 10.1007/s10207-023-00680-4

[77] Kaur, S., Kumar, K., Aggarwal, N.: Enhancing DDoS defense in SDN using hierarchical machine learning models. Journal of Network and Computer Applications **239**, 104168 (2025). DOI 10.1016/j.jnca.2025.104168

[78] Kavitha, D., Ramalakshmi, R.: Machine learning-based DDOS attack detection and mitigation in SDNs for IoT environments. Journal of the Franklin Institute **361**(17), 107197 (2024). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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 cybertwins architecture in IIoT-based smart airports. IEEE Transactions on Intelligent Transportation Systems **24**(2), 2368–2381 (2023). DOI 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). DOI 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). DOI 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). DOI 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). URL `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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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). DOI 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. Computers and Electrical Engineering **126**, 110485 (2025). DOI 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). DOI 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). DOI 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). DOI 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. International Journal of Critical Infrastructure Protection **47**, 100716 (2024). DOI 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). DOI 10.1109/DSN-S58398.2023.00024

[107] Mayer, K., Landauer, M., Skopik, F., Wurzenberger, M.: Engineering cyber ranges and security testbeds: A survey of technologies, use cases, and research trends. International Journal of Information Security (2026). Accepted, forthcoming

[108] 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). DOI 10.1109/ICICAT62666.2024.10923460

[109] 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). DOI 10.1109/ACCESS.2024.3375401

[110] 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 Networks **174**, 103840 (2025). DOI 10.1016/j.adhoc.2025.103840

[111] 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). DOI 10.1016/j.jlamp.2024.100965

[112] Moustafa, N.: A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society **72**, 102994 (2021). DOI 10.1016/j.scs.2021.102994

[113] 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). DOI 10.1109/ISEA-ISAP49340.2020.235010

[114] Mushi, M., Liu, Y., Sreenivasa, S., Ozdemir, O., Guvenc, I., Sichitiu, M., Dutta, R., Gyurek, R.: Open RAN testbeds with controlled air mobility. Computer Communications **228**, 107955 (2024). DOI 10.1016/j.comcom.2024.107955

[115] 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). DOI 10.1109/SmartGridComm57358.2023.10333908

[116] 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). DOI 10.1109/TSG.2024.3393439

[117] 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). DOI 10.1145/3470481.3472708

[118] 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). DOI 10.1109/ACCESS.2021.3101245

[119] National Initiative for Cybersecurity Education (NICE): Cyber ranges. One Pager (2018)

[120] 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). DOI 10.1145/3384217.3385623

[121] 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). DOI 10.1145/3626252.3630836

[122] Nguyen, H.P.T., Hasegawa, K., Fukushima, K., Beuran, R.: PenGym: Realistic training environment for reinforcement learning pentesting agents. Computers & Security **148**, 104140 (2025). DOI 10.1016/j.cose.2024.104140

[123] 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). DOI 10.1109/IAS54024.2023.10406799

[124] Nguyen, T.T., Kadavil, R., Hooshyar, H.: A real-time cyber-physical simulation testbed for cybersecurity assessment of large-scale power systems. IEEE Transactions on Industry Applications **60**(6), 8329–8340 (2024). DOI 10.1109/TIA.2024.3457877

[125] 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). DOI 10.1145/3641554.3701834

[126] 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). DOI 10.1145/3368308.3415364

[127] 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). DOI 10.1109/SOLI60636.2023.10425741

[128] 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). DOI 10.1109/ISCTURKEY53027.2021.9654352

[129] Palumickas, M., Yamin, M.M., Katt, B., Lal, C.: Evaluating ASCERT: Generative AI for cyber-range scenario generation. International Journal of Information Security **25**(1), 8 (2025). DOI 10.1007/s10207-025-01179-w

[130] 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). DOI 10.1016/j.iot.2025.101729

[131] 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). DOI 10.1145/3708821.3736186

[132] 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). DOI 10.1109/ISORC49007.2020.00022

[133] 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). DOI 10.1109/BigData62323.2024.10825128

[134] 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). DOI 10.1016/j.atech.2024.100727

[135] 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). DOI 10.1109/DASC55683.2022.9925750

[136] Purves, T., Kyriakopoulos, K.G., Jenkins, S., Phillips, I., Dudman, T.: Causally aware reinforcement learning agents for autonomous cyber defence. Knowledge-Based Systems **304**, 112521 (2024). DOI 10.1016/j.knosys.2024.112521

[137] 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). DOI 10.1145/3465481.3469185

[138] Qian, Y., Xie, H., Zhong, J., Chen, C., Bie, Z.: Resource allocation for hybrid quantum-classical communication systems in multiapplication-enabled power grids. IEEE Transactions on Industrial Informatics **21**(1), 267–276 (2025). DOI 10.1109/TII.2024.3452197

[139] 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). DOI 10.1109/ICCECT57938.2023.10141361

[140] 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 Transactions on Industry Applications **61**(3), 4566–4577 (2025). DOI 10.1109/TIA.2025.3549413

[141] 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). DOI 10.1145/3722573.3727830

[142] 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). DOI 10.1016/j.cose.2025.104323

[143] 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. Computer Networks **267**, 111364 (2025). DOI 10.1016/j.comnet.2025.111364

[144] Ravikumar, G., Hyder, B., Govindarasu, M.: Efficient modeling 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). DOI 10.1109/TD39804.2020.9299665

[145] Ravikumar, G., Hyder, B., Govindarasu, M.: Next-generation CPS testbed-based grid exercise - synthetic grid, attack, and defense modeling. In: 2020 Resilience Week (RWS), pp. 92–98 (2020). DOI 10.1109/RWS50334.2020.9241284

[146] 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). DOI 10.1109/WoWMoM54355.2022.00088

[147] 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). DOI 10.1109/IECON55916.2024.10905899

[148] 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). DOI 10.1109/CIEES62939.2024.10811376

[149] 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). DOI 10.1109/SmartGridComm57358.2023.10333893

[150] 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). DOI 10.1109/FiCloud58648.2023.00058

[151] Russo, E., Costa, G., Armando, A.: Building next generation cyber ranges with CRACK. Computers & Security **95**, 101837 (2020). DOI 10.1016/j.cose.2020.101837

[152] 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). DOI 10.1145/3617553.3617888

[153] 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). DOI 10.1016/j.jisa.2024.103956

[154] 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). DOI 10.1109/OAJPE.2024.3489477

[155] 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). DOI 10.1109/ICBIR57571.2023.10147612

[156] 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). DOI 10.1016/j.ijepes.2023.109735

[157] Sarkar, S., Teo, Y.M., Chang, E.C.: A cybersecurity assessment framework for virtual operational technology in power system automation. Simulation Modelling Practice and Theory **117**, 102453 (2022). DOI 10.1016/j.simpat.2021.102453

[158] 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). DOI 10.1109/MSCPES49613.2020.9133689

[159] 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). DOI 10.1109/DMC62632.2024.10812169

[160] Shahrouz, J.K., Analoui, M.: Privacy-aware revocation in VANETs with a Blockchain using accumulator. Vehicular Communications **53**, 100918 (2025). DOI 10.1016/j.vehcom.2025.100918

[161] 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. Future Generation Computer Systems **127**, 297–308 (2022). DOI 10.1016/j.future.2021.09.018

[162] 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). DOI 10.1109/ICPECA51329.2021.9362692

[163] 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). DOI 10.1109/ComPE53109.2021.9752401

[164] 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). DOI 10.1109/IATMSI60426.2024.10502505

[165] 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). DOI 10.1109/IATMSI56455.2022.10119321

[166] 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). DOI 10.1109/STPEC52385.2021.9718616

[167] Silva, M., Pinto, D., Vitorino, J., Gonçalves, J., Maia, E., Praça, I.: GeNIS: A modular dataset for network intrusion detection and classification. Data in Brief **60**, 111487 (2025). DOI 10.1016/j.dib.2025.111487

[168] 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

[169] Sipola, T., Kokkonen, T., Puura, M., Riuttanen, K.E., Pitkäniemi, K., Juutilainen, E., Kontio, T.: Digital Twin of Food Supply Chain for Cyber Exercises. Applied Sciences **13**(12), 7138 (2023). DOI 10.3390/app13127138

[170] 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). DOI 10.1016/j.procir.2020.03.007

[171] 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). DOI 10.1109/PESGM51994.2024.10689146

[172] Sun, N., Wang, W., Liu, K., Li, D., Lü, J.: Hybrid framework for security evaluation in Internet of Vehicles. Computers & Security **153**, 104398 (2025). DOI 10.1016/j.cose.2025.104398

[173] 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). DOI 10.1016/j.vehcom.2024.100822

[174] 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). DOI 10.1109/DMC62632.2024.10812136

[175] Syed, A., Nour, B., Pourzandi, M., Assi, C., Debbabi, M.: Comprehensive advanced persistent threats dataset. IEEE Networking Letters **7**(2), 150–154 (2025). DOI 10.1109/LNET.2025.3551989

[176] 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). DOI 10.1109/TPEC63981.2025.10906863

[177] 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). DOI 10.1109/CANDARW57323.2022.00023

[178] 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). DOI 10.1109/TCCN.2025.3539660

[179] 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). DOI 10.1145/3474718.3474725

[180] 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). DOI 10.1109/CANDARW53999.2021.00073

[181] 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). DOI 10.1109/CARS61786.2024.10778886

[182] 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). DOI 10.1145/3546096.3546115

[183] 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). DOI 10.1145/3697090.3699870

[184] Torquato, M., Maciel, P., Vieira, M.: Evaluation of time-based virtual machine migration as moving target defense against host-based attacks. Journal of Systems and Software **219**, 112222 (2025). DOI 10.1016/j.jss.2024.112222

[185] 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). DOI 10.1016/j.jisa.2025.104199

[186] 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). DOI 10.1145/3675741.3675751

[187] 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). DOI 10.1016/j.cose.2025.104566

[188] Uçtu, G., Alkan, M., Doğru, İ.A., Dörterler, M.: A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls. Future Generation Computer Systems **124**, 56–67 (2021). DOI 10.1016/j.future.2021.05.013

[189] 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). DOI 10.1145/3485832.3488020

[190] 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). DOI 10.3390/s20247148

[191] 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). DOI 10.1109/Cyber-RCI60769.2024.10939197

[192] Vashishtha, L.K., Chatterjee, K.: Strengthening cybersecurity: TestCloudIDS dataset and SparkShield algorithm for robust threat detection. Computers & Security **151**, 104308 (2025). DOI 10.1016/j.cose.2024.104308

[193] 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). DOI 10.1109/EEITE61750.2024.10654399

[194] 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 Transactions on Learning Technologies **14**(3), 322–337 (2021). DOI 10.1109/TLT.2021.3091904

[195] 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). DOI 10.1145/3714393.3726006

[196] 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). DOI 10.1109/ICECET61485.2024.10698747

[197] 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). DOI 10.1016/j.cose.2025.104449

[198] 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). DOI 10.1145/3701233

[199] 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). DOI 10.1145/3711900

[200] 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). DOI 10.1016/j.gloei.2021.05.004

[201] 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). DOI 10.1016/j.cose.2024.104114

[202] 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)

[203] 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). DOI 10.1145/3703159

[204] 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). DOI 10.1109/EuroSPW54576.2021.00032

[205] 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). DOI 10.1145/3546096.3546111

[206] 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). DOI 10.1109/LCN53696.2022.9843801

[207] Yamin, M.M., Katt, B.: Modeling and executing cyber security exercise scenarios in cyber ranges. Computers & Security **116**, 102635 (2022). DOI 10.1016/j.cose.2022.102635

[208] Yamin, M.M., Katt, B.: Use of cyber attack and defense agents in cyber ranges: A case study. Computers & Security **122**, 102892 (2022). DOI 10.1016/j.cose.2022.102892

[209] Yamin, M.M., Katt, B., Gkioulos, V.: Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security **88**, 101636 (2020). DOI 10.1016/j.cose.2019.101636

[210] 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). DOI 10.1109/ICACS69208.2026.11433152

[211] 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). DOI 10.1109/ITEC48692.2020.9161525

[212] 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). DOI 10.1016/j.vehcom.2023.100649

[213] Zacharis, A., Patsakis, C.: AiCEF: An AI-assisted Cyber Exercise Content Generation Framework Using Named Entity Recognition (2022). DOI 10.48550/arXiv.2211.10806

[214] 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). DOI 10.1109/APEIE59731.2023.10347585

[215] 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). DOI 10.1109/CNS62487.2024.10735649

[216] 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). DOI 10.1109/MCOM.002.2400601

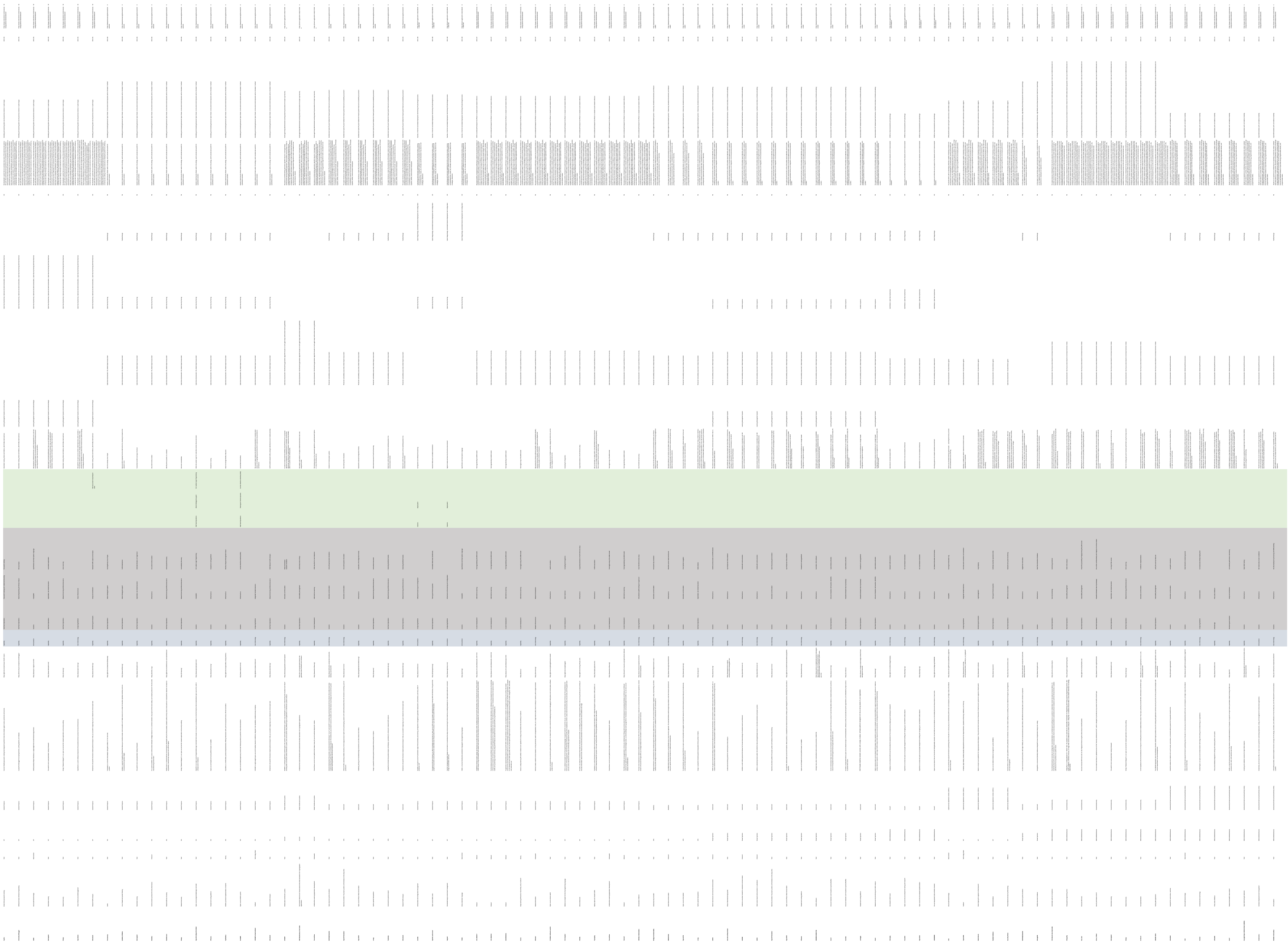
[217] Zhang, Y., Liu, Z., Jia, C., Zhu, Y., Miao, C.: An online defense against object-based LiDAR attacks in autonomous driving. In: Proceedings of the 22nd ACM Conference on Embedded Networked Sensor Systems, pp. 380–393. ACM, Hangzhou China (2024). DOI 10.1145/3666025.3699345

[218] 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). DOI 10.1109/MCE.2022.3203202

[219] 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). DOI 10.1145/3702163.3702183

Technology Name	Technology Intended Purpose	Technology Type	CR & TB Application Domain	CR & TB Application Subdomain
Docker	Containerisation technology	Tool	RAN & Mobile Devices	5G and 6G Security
Hydra	Brute-force password-cracking	Tool	RAN & Mobile Devices	5G and 6G Security
MySQL Database	Relational database	Tool	RAN & Mobile Devices	5G and 6G Security
Nmap	Network discovery	Tool	RAN & Mobile Devices	5G and 6G Security
OAI 5G core	5G implementation	Tool	RAN & Mobile Devices	5G and 6G Security
OAI's gNB emulator	5G software stack	Technology Stack	RAN & Mobile Devices	5G and 6G Security
DETERLab	Testbed	Technology Stack	Power Systems	Power System Automation
Hping	TCP/IP packet generator	Tool	Power Systems	Power System Automation
Metasploit	Penetration testing	Tool	Power Systems	Power System Automation
Modbus	Communication protocol for industrial devices	Protocol	Power Systems	Power System Automation
Nmap	Network discovery	Tool	Power Systems	Power System Automation
PowerWorld	Power system simulation	Tool	Power Systems	Power System Automation
ScadaBR	Open-source SCADA system	Tool	Power Systems	Power System Automation
Zabbix	Network and system monitoring	Tool	Power Systems	Power System Automation
GOOSE	Publisher-subscriber model for substation communication	Protocol	Power Systems	Electrical substations
IEC61850 open server	IED implementation	Tool	Power Systems	Electrical substations
Nmap	Network discovery	Tool	Power Systems	Electrical substations
Proxmox VE	Virtualization Platform	Tool	Power Systems	Electrical substations
RSCAD simulation software	Cyber-physical system simulation	Tool	Power Systems	Electrical substations
RTDS simulator	Real-time power system simulation	Tool	Power Systems	Electrical substations
SV	Industrial Communication	Protocol	Power Systems	Electrical substations
Wireshark	Network Traffic Analysis	Tool	Power Systems	Electrical substations
CICFlowMeter	Generates and analyzes network traffic	Tool	Power Systems	Electrical substations
CSV	Structured Data Exchange	Data Format	Power Systems	Electrical substations
GOOSE	Publisher-subscriber model for substation communication	Protocol	Power Systems	Electrical substations
IEC 60870-5-104	Smart Grid Communication	Protocol	Power Systems	Electrical substations
Sampled Values	Industrial Communication	Protocol	Power Systems	Electrical substations
Tcpdump	Command-line packet analyzer	Tool	Power Systems	Electrical substations
Tshark	Network Traffic Analysis	Tool	Power Systems	Electrical substations
VyOS	Open source network operating system	OS	Power Systems	Electrical substations
MANO	Management and orchestration for NFV	Tool	Intelligent Transportation Systems	In-vehicle Security
OpenStack	Cloud Infrastructure & Management	Tool	Intelligent Transportation Systems	In-vehicle Security
Apache Kafka	Distributed event streaming platform	Tool	RAN & Mobile Devices	5G and 6G Security
Elastic Logstash	Log collection, storage, and search	Tool	RAN & Mobile Devices	5G and 6G Security
Elasticsearch	Data store and search engine	Tool	RAN & Mobile Devices	5G and 6G Security
Esper	Complex event processing (CEP) and streaming analytics	Tool	RAN & Mobile Devices	5G and 6G Security
JSON	Structured Data Exchange	Data Format	RAN & Mobile Devices	5G and 6G Security
Kafka SQL	Non-relational database	Tool	RAN & Mobile Devices	5G and 6G Security
Keras	Deep learning API built on TensorFlow, JAX, or PyTorch	Library	RAN & Mobile Devices	5G and 6G Security
MATILDA testbed	Testbed	Technology Stack	RAN & Mobile Devices	5G and 6G Security
Mouseworld testbed	Testbed	Technology Stack	RAN & Mobile Devices	5G and 6G Security
Siddhi	Cloud-native CEP system for real-time analytics	Tool	RAN & Mobile Devices	5G and 6G Security
TensorFlow	AI & Machine Learning Application Development	Framework	RAN & Mobile Devices	5G and 6G Security
GOOSE	Publisher-subscriber model for substation communication	Protocol	CPS	Electrical substations
libIEC61850	Developing IEC 61850-compliant devices	Library	CPS	Electrical substations
Tshark	Network Traffic Analysis	Tool	CPS	Electrical substations
Common Industrial Protocol (CIP)	Industrial Communication Protocol	Protocol	ICS	Nuclear Power Plant
Rockwell Automation's FactoryTalk Linx software	Industrial communication platform	Tool	ICS	Nuclear Power Plant
Rockwell studio 5000 logix designer software	Programming software for industrial control systems.	Tool	ICS	Nuclear Power Plant
Western Services Corporation (WSC) Generic Pressurized Water Reactor (GPWR)	Pressurized Water Reactor Simulator	Tool	ICS	Nuclear Power Plant
WSC 3keymaster	Simulation Platform	Tool	ICS	Nuclear Power Plant
Modbus	Communication protocol for industrial devices	Protocol	CPS	Industrial Cyber-Physical Systems
MulVAL	Vulnerability analysis	Tool	CPS	Industrial Cyber-Physical Systems
Siemens windows control center (WinCC)	SCADA system for process visualization	Tool	CPS	Industrial Cyber-Physical Systems
DIGSI4	Engineering Software	Tool	Power Systems	Smart Grid
EMTP-ATP	Simulating electromagnetic transients	Tool	Power Systems	Smart Grid
ETAP software	Electrical power system analysis	Tool	Power Systems	Smart Grid
aireplay-ng	Cracking the WEP and WPA-PSK keys	Tool	Power Systems	Smart Grid
Airgeddon	Audit wireless networks	Tool	Power Systems	Smart Grid
Amazon Web Services (AWS)	Cloud computing services	Platform	Power Systems	Smart Grid
AWS Grafana	Systems monitoring and alerting	Tool	Power Systems	Smart Grid
AWS NoSQL DB	Nosql database	Tool	Power Systems	Smart Grid
Azure Digital Twins	DT Platform as a service (PaaS)	Tool	Power Systems	Smart Grid
CSV	Structured Data Exchange	Data Format	Power Systems	Smart Grid
Ettercap	Man in the middle attacks	Tool	Power Systems	Smart Grid
Google Colab	Browser-based IDE	Tool	Power Systems	Smart Grid
Hping	TCP/IP packet generator	Tool	Power Systems	Smart Grid
MySQL Database	Relational database	Tool	Power Systems	Smart Grid
Nmap	Network discovery	Tool	Power Systems	Smart Grid
Sqlmap	SQL injection	Tool	Power Systems	Smart Grid
Wireshark	Network Traffic Analysis	Tool	Power Systems	Smart Grid
Xprobe2	Fingerprinting tool	Tool	Power Systems	Smart Grid
Cewl	Custom wordlist generation	Tool	IoT, IIoT	AI-based IoT Security
CSV	Structured Data Exchange	Data Format	IoT, IIoT	AI-based IoT Security
DVWA	Vulnerable web application	Tool	IoT, IIoT	AI-based IoT Security
Hydra	Brute-force password-cracking	Tool	IoT, IIoT	AI-based IoT Security
Metasploit	Penetration testing	Tool	IoT, IIoT	AI-based IoT Security
Metasploitable	Vulnerable VM	Tool	IoT, IIoT	AI-based IoT Security
MQTT	IoT Messaging protocol	Protocol	IoT, IIoT	AI-based IoT Security
Nessus	Vulnerability Scanner	Tool	IoT, IIoT	AI-based IoT Security
Netsniff-ng	Linux networking toolkit	Tool	IoT, IIoT	AI-based IoT Security
Nmap	Network discovery	Tool	IoT, IIoT	AI-based IoT Security
Node-RED	Flow-based programming	Tool	IoT, IIoT	AI-based IoT Security
Ostinato	Traffic generation	Tool	IoT, IIoT	AI-based IoT Security
OWASP security Shepherd VM	Vulnerable VM	Tool	IoT, IIoT	AI-based IoT Security
scapy	Python packet manipulation	Library	IoT, IIoT	AI-based IoT Security

LightGBM	Gradient boosting framework	Library	ICS	Industrial IoT Security	LightGBM is a gradient boosting framework that uses tree based learning algorithms. It is designed to be distributed and efficient with the following advantages: Faster training speed and higher efficiency. Lower memory usage. Better accuracy. Support of parallel, distributed, and GPU learning. Capable of handling large-scale data.	https://lightgbm.readthedocs.io/en/stable/	Capability	Custom Development	AI & Machine Learning	Industrial data forecast			
Modbus	Communication protocol for industrial devices	Protocol	ICS	Industrial IoT Security	It is used to establish client-server communication between intelligent devices. It is a de facto standard, truly open and the most widely used network protocol in the industrial manufacturing environment.	https://modbus.org/	Capability	Scenario	Infrastructure	Multi-vendor PLC communication			
OPC Unified Architecture (OPC-UA)	Communication protocol for industrial devices	Protocol	ICS	Industrial IoT Security	The OPC Unified Architecture (UA), released in 2008, is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework.	https://opcfoundation.org/about/opc-technologies/opc-ua/	Capability	Scenario	Infrastructure	Industrial Communication			
Unity3D	Game Development and Simulation	Tool	ICS	Industrial IoT Security	Unity's industry-leading engine provides tools to create and run amazing games and other real-time interactive experiences and publish to a variety of devices.	https://unity.com/	Capability	Scenario	Simulation and Emulation	Digital twin simulation			
CSV	Structured Data Exchange	Data Format	CPS	Manufacturing Systems	CSV is one of the most popular formats for publishing data on the web. It is concise, easy to understand by both humans and computers, and aligns nicely to the tabular nature of most data.	https://www.w3.org/2013/csvw/wiki/Main_Page.html	Capability	Custom Development	Dataset Generation	Structured data exchange format for Dataset			
Factory I/O	3D factory simulation	Tool	CPS	Manufacturing Systems	Factory I/O is a 3D factory simulation for learning automation technologies. Designed to be easy to use, it allows to quickly build a virtual factory using a selection of common industrial parts.	https://factoryio.com/	Capability	Scenario	Simulation and Emulation	Simulate manufacturing process			
Google Colab	Browser-based IDE	Tool	CPS	Manufacturing Systems	With Colab or "Colaboratory," you can write and run Python code in your browser. You can do the following: No configuration required; Free access to GPUs; Easy sharing;	https://colab.research.google.com/	Capability	Custom Development	AI & Machine Learning	Implementation of deep learning model			
OpenPLC	Open-source programmable logic controller	Tool	CPS	Manufacturing Systems	OpenPLC is an open-source Programmable Logic Controller that is based on an easy to use software. It is the first fully functional standardized open source PLC, both in software and in hardware.	https://www.openplcproject.com/	Capability	Scenario	Infrastructure	Simulation of control logic on sensors and actuators			
sktime	Framework for ML and AI with time series	Library	CPS	Manufacturing Systems	An easy-to-use, easy-to-extend, comprehensive python framework for ML and AI with time series	https://www.sktime.net/en/stable/	Capability	Custom Development	AI & Machine Learning	Training and benchmarking of time series classification models			
Android Emulator	Android Emulator	Tool	RAN & Mobile Devices	Android Devices	The Android Emulator simulates Android devices on your computer so that you can test your application on a variety of devices and Android API levels without needing to have each physical device.	https://developer.android.com/studio/run/emulator	Capability	Scenario	Simulation and Emulation	Mobile Platform Simulation			
Docker	Containerisation technology	Tool	RAN & Mobile Devices	Android Devices	Docker Engine is an open source Containerisation technology for building and containerizing your applications.	https://www.docker.com/	Core Technology	Computing Platform	Containerisation	Setting up and isolating Android instances and attacker services			
Ghidra	Reverse engineering (SRE) framework	Tool	RAN & Mobile Devices	Android Devices	Ghidra is a software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate	https://github.com/NationalSecurityAgency/ghidra	Capability	Red Team Operations	Reverse Engineering and Binary Analysis	Reverse engineering for target analysis			
Gophish	Open-source phishing framework	Tool	RAN & Mobile Devices	Android Devices	Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.	https://getgophish.com/	Capability	Red Team Operations	Phishing and Social Engineering	Phishing campaign simulation			
iOS Simulator	iOS Simulator	Tool	RAN & Mobile Devices	Android Devices	Launch your app in a simulated iOS, tvOS, watchOS, or visionOS device, or on a device connected to a Mac.	https://developer.apple.com/documentation/xcode/running-your-app-in-simulator-or-on-a-device	Capability	Scenario	Simulation and Emulation	Mobile Platform Simulation			
Nginx Web server	HTTP server, reverse proxy, and load balancer	Tool	RAN & Mobile Devices	Android Devices	nginx ("engine x") is an HTTP web server, reverse proxy, content cache, load balancer, TCP/UDP proxy server, and mail proxy server.	https://nginx.org/	Capability	Scenario	Infrastructure	Backend Module: Webserver			
Node.js	JavaScript runtime environment	Framework	RAN & Mobile Devices	Android Devices	Node.js® is a free, open-source, cross-platform JavaScript runtime environment that lets developers create servers, web apps, command line tools and scripts.	https://nodejs.org/	Capability	Custom Development	Backend Frameworks	Backend Module			
React.js	Web and native user interfaces	Library	RAN & Mobile Devices	Android Devices	The library for web and native user interfaces. React is a library. It lets you put components together, but it doesn't prescribe how to do routing and data fetching. To build an entire app with React, we recommend a full-stack React framework like Next.js or Remix.	https://react.dev/	Capability	Custom Development	Frontend Frameworks	UI component			
scrcpy	Screen mirroring and remote control of Android devices	Tool	RAN & Mobile Devices	Android Devices	This application mirrors Android devices (video and audio) connected via USB or over TCP/IP, and allows to control the device with the keyboard and the mouse of the computer. It does not require any root access. It works on Linux, Windows and macOS.	https://github.com/Genymobile/scrcpy	Capability	Portal Services	User Access	Virtual display synchronization	Monitoring and Analytics	Visualization & Dashboarding	Virtual display synchronization
websockify	WebSockets-to-TCP proxy	Tool	RAN & Mobile Devices	Android Devices	At the most basic level, websockify just translates WebSockets traffic to normal socket traffic. Websockify accepts the WebSockets handshake, parses it, and then begins forwarding traffic between the client and the target in both directions.	https://github.com/novnc/websockify	Capability	Portal Services	User Access	VNC-to-WebSocket conversion	Monitoring and Analytics	Visualization & Dashboarding	VNC-to-WebSocket conversion
Wi-Fi Baby Monitor	Baby monitoring system	Tool	RAN & Mobile Devices	Android Devices	N/A	N/A	Capability	Red Team Operations	Training and Practice Systems	Mobile device Threat and vulnerability assessment			
x11vnc	VNC server	Tool	RAN & Mobile Devices	Android Devices	x11vnc allows one to view remotely and interact with real X displays (i.e. a display corresponding to a physical monitor, keyboard, and mouse) with any VNC viewer. In this way it plays the role for Unix/X11 that WinVNC plays for Windows.	https://github.com/LibVNC/x11vnc	Capability	Portal Services	User Access	Virtual display synchronization	Monitoring and Analytics	Visualization & Dashboarding	Virtual display synchronization
9p	Remote filesystem protocol	Protocol	ICT	General Purpose	Unix implementation of the Plan 9 9p remote filesystem protocol.	https://github.com/sbl/9p/	Capability	Management	Platform & Environment Management	Transparent File System Mapping			
Docker	Containerisation technology	Tool	ICT	General Purpose	Docker Engine is an open source Containerisation technology for building and containerizing your applications.	https://www.docker.com/	Core Technology	Computing Platform	Containerisation	Infrastructure Provisioning and Configuration			
Gdb	GNU debugger	Tool	ICT	General Purpose	Debugger: GDB, the GNU Project debugger, allows you to see what is going on 'inside' another program while it executes -- or what another program was doing at the moment it crashed.	https://www.sourceware.org/gdb/	Capability	Custom Development	Debugger	Tool for Security Exercise Environment			
Gef	GDB extension for exploit development	Tool	ICT	General Purpose	GEF is a set of commands for x86/64, ARM, MIPS, PowerPC and SPARC to assist exploit developers and reverse-engineers when using old school GDB	https://github.com/hugsy/gef	Capability	Custom Development	Debugger	Tool for Security Exercise Environment			
Ghidra	Reverse engineering (SRE) framework	Tool	ICT	General Purpose	Ghidra is a software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate	https://github.com/NationalSecurityAgency/ghidra	Capability	Blue Team Operations	Reverse Engineering and Binary Analysis	Tool for Security Exercise Environment			
Ipython	Interactive Python shell	Tool	ICT	General Purpose	IPython provides a rich toolkit to help you make the most of using Python interactively.	https://ipython.org/	Capability	Custom Development	Integrated Development Environment	Tool for Security Exercise Environment			
Nmap	Network discovery	Tool	ICT	General Purpose	Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.	https://nmap.org/	Capability	Red Team Operations	Network Scanning and Reconnaissance	Tool for Security Exercise Environment			
OpenSSH	Secure remote login	Tool	ICT	General Purpose	OpenSSH is the premier connectivity tool for remote login with the SSH protocol.	https://www.openssh.com/	Capability	Portal Services	User Access	Student Environment Access			
Pwndbg	GDB extension for exploit development	Tool	ICT	General Purpose	GDB plug-in that makes debugging with GDB suck less, with a focus on features needed by low-level software developers, hardware hackers, reverse-engineers and exploit developers.	https://github.com/pwndbg/pwndbg	Capability	Red Team Operations	Attack Strategy & Support	Tool for Security Exercise Environment			
Pwntools	Enhanced debugging	Tool	ICT	General Purpose	Pwntools is a CTF framework and exploit development library.	https://github.com/Gallopsled/pwntools	Capability	Red Team Operations	Exploitation and Attack Execution	Tool for Security Exercise Environment			
QEMU	Machine emulator and virtualizer	Tool	ICT	General Purpose	A generic and open source machine emulator and virtualizer	https://www.qemu.org/	Capability	Computing Platform	Virtualization platform/Type-2-Hypervisor				
Radare2	Reverse engineering (SRE) framework	Tool	ICT	General Purpose	Radare is a portable reversing framework	https://rada.re/n/	Capability	Blue Team Operations	Reverse Engineering and Binary Analysis	Tool for Security Exercise Environment			
scapy	Python packet manipulation	Library	ICT	General Purpose	Scapy is a powerful interactive packet manipulation library written in Python.	https://scapy.net/	Capability	Red Team Operations	Paketmanipulation	Tool for Security Exercise Environment			
SLIRP	Network Emulation	Tool	ICT	General Purpose	Software program that emulates a PPP, SLIP, or CSLIP connection to the Internet via a shell account.	https://github.com/kost/slirp	Capability	Scenario	Infrastructure	VM-Container Networking			
Strace	System call tracer for Linux	Tool	ICT	General Purpose	strace is a diagnostic, debugging and instructional userspace utility for Linux. It is used to monitor and tamper with interactions between processes and the Linux kernel, which include system calls, signal deliveries, and changes of process state.	https://strace.io/	Capability	Monitoring and Analytics	Analysis & Verification	Tool for Security Exercise Environment			
Tmux	Terminal multiplexer	Tool	ICT	General Purpose	Terminal Multiplexer: Tmux is a program which runs in a terminal and allows multiple other terminal programs to be run inside it.	https://github.com/tmux/tmux/wiki	Capability	Portal Services	User Access	Tool for Security Exercise Environment			
VS Code	open-source code editor	Tool	ICT	General Purpose	VS Code is a lightweight, open-source code editor developed by Microsoft	https://code.visualstudio.com/	Capability	Portal Services	User Access	Student Environment Access			
Wireshark	Network Traffic Analysis	Tool	ICT	General Purpose	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Blue Team Operations	Network Analysis & Reconnaissance	Tool for Security Exercise Environment			
HYPERSIM	Real-time simulation platform for power systems	Tool	Intelligent Transportation Systems	Electric vehicle charging stations	HYPERSIM is the world's most advanced real-time simulation platform for power systems, combining hardware-in-the-loop (HIL), software-in-the-loop (SIL), and offline simulation acceleration in a single, high-performance environment. As a leading power system real time simulator, our platform provides a robust environment for accurate power system simulation and power systems testing. Built by engineers for engineers, it empowers users to model, test, and validate complex electrical grids and inverter-based resource (IBR) integration with unmatched speed and precision.	https://www.opal-rt.com/software-platforms/hypersim/	Core Technology	Scenario	Simulation and Emulation	Model the power grid			
MATLAB/Simulink	Cyber-physical system simulation	Tool	Intelligent Transportation Systems	Electric vehicle charging stations	Simulink Desktop Real-Time provides a real-time kernel for Windows, Linux, and macOS. It includes drag-and-drop Simulink I/O driver blocks that enable closed-loop control of physical systems from your desktop computer. The toolbox lets you connect to sensors, actuators, and other devices to prototype and test control systems without requiring dedicated real-time test equipmen	https://www.mathworks.com/products/simulink-desktop-real-time.html	Capability	Scenario	Simulation and Emulation	Modelling IEEE New England 39-bus system			
OpalTarget OP5707XG	Real-time digital simulator	Tool	Intelligent Transportation Systems	Electric vehicle charging stations	The OP5707XG real-time digital simulator offers an unequaled level of FPGA performance and optical connectivity to meet top-level requirements. It's an all-in-one solution that combines the latest Intel® Xeon® processing cores with the power of a AMD Virtex™-7 FPGA, while supporting an extensive list of communication protocols to meet the requirements of the most demanding hardware-in-the-loop (HIL) and rapid control prototyping (RCP) applications.	https://www.opal-rt.com/hardware/simulators/real-time-simulators/op5707xg/	Capability	Scenario	Simulation and Emulation	Implementation of HYPERSIM models			
Open Charge Point Protocol (OCPP)	Standard for EV charging stations	Protocol	Intelligent Transportation Systems	Electric vehicle charging stations	The goal of the Open Charge Point Protocol (OCPP) is to provide a uniform method of communication between charge points and central systems. This protocol makes it possible to connect any central system with any charge point, regardless of the vendor. A uniform approach helps prevent coordination problems and therefore benefits the entire electric vehicle market.	https://openchargealliance.org/protocols/open-charge-point-protocol/	Capability	Scenario	Infrastructure	Charging station remote communication			
VMWare vSphere	Virtualization platform	Tool	Intelligent Transportation Systems	Electric vehicle charging stations	The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.	https://www.vmware.com/products/cloud-infrastructure/vsphere	Core Technology	Computing Platform	Virtualization platform/Type-1-Hypervisor				
aircrack-ng	Assess WiFi network security	Tool	ICT	Cloud Infrastructure	Aircrack-ng is a complete suite of tools to assess WiFi network security. All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily on Linux but also Windows, macOS, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.	https://www.aircrack-ng.org/doku.php?id=Main	Capability	Red Team Operations	Exploitation and Attack Execution	De-authentication Attack			
Airgeddon	Audit wireless networks	Tool	ICT	Cloud Infrastructure	This is a multi-use bash script for Linux systems to audit wireless networks.	https://github.com/v1s1t0r1sh3r3/airgeddon	Capability	Red Team Operations	Spoofing and Identity Deception	Evil Twin Attack			
Amazon Web Services (AWS)	Cloud computing services	Platform	ICT	Cloud Infrastructure	Amazon Web Services (AWS) is the world's most comprehensive and widely used cloud, with more than 200 services offering extensive functionality and delivered from globally distributed data centers.	https://aws.amazon.com/	Core Technology	Computing Platform	Cloud Infrastructure				
Arduino IDE	Development environment	Tool	ICT	Cloud Infrastructure	The Arduino IDE 2 is an improvement of the classic IDE, with increased performance, improved user interface and many new features, such as autocompletion, a built-in debugger and syncing sketches with Arduino Cloud.	https://www.arduino.cc/en/software/	Capability	Custom Development	Integrated Development Environment	IoT Devices			
CSV	Structured Data Exchange	Data Format	ICT	Cloud Infrastructure	CSV is one of the most popular formats for publishing data on the web. It is concise, easy to understand by both humans and computers, and aligns nicely to the tabular nature of most data.	https://www.w3.org/2013/csvw/wiki/Main_Page.html	Capability	Custom Development	Dataset Generation	Data Format for Network Traffic			
Ettercap	Man in the middle attacks	Tool	ICT	Cloud Infrastructure	Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.	https://www.ettercap-project.org/	Capability	Red Team Operations	Paketmanipulation	ARP poisoning attack			
Flower Framework	Federated AI Framework	Framework	ICT	Cloud Infrastructure	Flower (Flwr) is a framework for building federated AI systems. The design of Flower is based on a few guiding principles:	https://github.com/adap/flower	Capability	Custom Development	AI & Machine Learning	Large-scale FL simulations			
Grafana	Systems monitoring and alerting	Tool	ICT	Cloud Infrastructure	Grafana Open Source Software (OSS) enables you to query, visualize, alert on, and explore your metrics, logs, and traces wherever they're stored.	https://grafana.com/	Capability	Monitoring and Analytics	Visualization & Dashboarding	Sensor data visualization			
Hping	TCP/IP packet generator	Tool	ICT	Cloud Infrastructure	EMTP-ATP is the original electromagnetic transient program, it covers all range of transients from lightning and switching studies to temporary overvoltages and sub-synchronous resonance. It has steady-state initialization, good support for multi-conductor analysis, powerful scripting in MODELS.	https://www.atp-emtp.org/showpage.php?id=3	Capability	Red Team Operations	Network Scanning and Reconnaissance	Port Scanning			
MySQL Database	Relational database	Tool	ICT	Cloud Infrastructure	The MySQL software delivers a very fast, multithreaded, multi-user, and robust SQL (Structured Query Language) database server.	https://www.mysql.com/	Core Technology	Data Storage	Relational Database				
Nmap	Network discovery	Tool	ICT	Cloud Infrastructure	Nmap ("Network Mapper") is an open source tool for network exploration and security auditing.	https://nmap.org/	Capability	Red Team Operations	Network Scanning and Reconnaissance	Port scanning			
Sqlmap	SQL injection	Tool	ICT	Cloud Infrastructure	sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.	https://sqlmap.org/	Capability	Red Team Operations	Exploitation and Attack Execution	SQL injection			
Tracemalloc	Debug tool	Tool	ICT	Cloud Infrastructure	The tracemalloc module is a debug tool to trace memory blocks allocated by Python.	https://docs.python.org/3/library/tracemalloc.html	Capability	Scenario	Infrastructure	Tracking memory allocations			
Wireshark	Network Traffic Analysis	Tool	ICT	Cloud Infrastructure	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Monitoring and Analytics	Data Collection	Monitor WiFi traffic			
Xprobe2	Fingerprinting tool	Tool	ICT	Cloud Infrastructure	Xprobe2 is a remote active operating system fingerprinting tool. Xprobe2 uses advanced technics, such as the usage of fuzzy logic to match fingerprinting results with the tool's signature database, unique fingerprinting methods and other, to provide with accurate results.	https://github.com/binarytrails/xprobe2	Capability	Red Team Operations	Network Scanning and Reconnaissance	OS fingerprinting			
DNP3	Electric transmission and industrial communication	Protocol	CPS	IEC 61850 IED Modeling	DNP3 has grown to be the most widely used protocol for electric transmission and distribution communications in North America and other regions of the world, and is a named standard for DER communications. DNP3 is also broadly adopted in adjacent industries such as water / wastewater, transportation and the oil and gas industry.	https://www.dnp.org/	Capability	Scenario	Infrastructure	SCADA communication with the substation RTUs			
GOOSE	Publisher-subscriber model for substation communication	Protocol	CPS	IEC 61850 IED Modeling	GOOSE is an IEC 61850 protocol that allows for the real-time exchange of substation events over Ethernet.	https://iec61850.dvl.iec.ch/	Capability	Scenario	Infrastructure	IED and OPAL-RT simulator communication			
MMS	Client-server-based communication in substations	Protocol	CPS	IEC 61850 IED Modeling	MMS is a standard protocol within IEC 61850 for data exchange between devices in industrial automation and power systems.	https://iec61850.dvl.iec.ch/	Capability	Scenario	Infrastructure	IED and SICAM PAS in Substation-RTU communication			
Opal-RT Simulator	Real-time simulation for power systems and hardware-in-the-loop (HIL)	Tool	CPS	IEC 61850 IED Modeling	Real-time simulation platform for power systems and hardware-in-the-loop testing	https://www.opal-rt.com/	Capability	Scenario	Simulation and Emulation	Industrial Systems Simulation			
OpenPDC	Open-source Phasor Data Concentrator	Tool	CPS	IEC 61850 IED Modeling	The openPDC administered by the Grid Protection Alliance (GPA) is a complete Phasor Data Concentrator software system designed to process streaming time-series data in real-time.	https://github.com/GridProtectionAlliance/openPDC	Capability	Scenario	Simulation and Emulation	Software-based Phasor Data Concentrator (PDC)			
RT-LAB	Real-time simulation for power systems integrated with MATLAB/Simulink	Tool	CPS	IEC 61850 IED Modeling	Fully integrated with MATLAB/Simulink, RT-LAB enables Simulink models to interact with the real world in real-time. This makes RT-LAB an ideal software platform of real-time simulation for engineers to rapidly develop and validate their applications, regardless of their complexity. As a multi-domain platform, RT-LAB provides flexible and scalable solutions for the power systems, power electronics, aerospace, and automotive industries.	https://www.opal-rt.com/software-rt-lab/	Capability	Scenario	Simulation and Emulation	Map the desired physical IEDs to OPAL-RT			
SIEMENS SICAM PAS	SCADA software	Tool	CPS	IEC 61850 IED Modeling	r some years now, power generation and distribution have been undergoing major changes. The innovation cycles (where operating equipment and communication media are concerned) are getting ever shorter, and the market is becoming increasingly deregulated. The systems used to monitor power supply equipment and processes must take account of these changes. When new products are used, user friendliness, easy engineering, manifold interfacing to various communication media and extensibility are important Features. SICAM PAS (Power Automation System) meets all the demands placed on a distributed substation control system – both now and in the future. Amongst many other standardized communication protocols, SICAM PAS particularly supports the IEC 61850 standard for communication between substations and IEDs. SICAM PAS is an open system and – in addition to standardized data transfer processes – it features user interfaces for the integration of system-specific tasks and offers multiple automation options. SICAM PAS can thus be easily included in existing systems and used for system integration, too. With modern diagnostics, it optimally supports commissioning and maintenance. SICAM PAS is clearly structured and reliable, thanks to its open, fully documented and tested System.	https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/substation-automation/substation-automation-system-sicam-pas.html	Capability	Scenario	Infrastructure	SCADA substation remote terminal unit (RTU)			
VMWare	Type-2 Hypervisor	Tool	CPS	IEC 61850 IED Modeling	The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.	https://www.vmware.com/products/cloud-infrastructure/vsphere	Core Technology	Computing Platform	Virtualization platform/Type-2-Hypervisor	Infrastructure Provisioning and Configuration			
KVM	Virtualization Platform	Tool	IoT, IIoT	Cloud Infrastructure	KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.	https://linux-kvm.org/page/Main_Page	Core Technology	Computing Platform	Virtualization platform/Type-1-Hypervisor				
Memtester	Memory subsystem testing	Tool	IoT, IIoT	Cloud Infrastructure	Memtester is an effective userspace tester for stress-testing the memory subsystem. It is very effective at finding intermittent and non-deterministic faults.	https://linux.die.net/man/8/memtester	Capability	Scenario	Infrastructure	Benchmarking / Stress Testing			
Mosquitto MQTT Broker	MQTT broker	Tool	IoT, IIoT	Cloud Infrastructure	Eclipse Mosquitto is an open source (EPL/EDL licensed) message broker that implements the MQTT protocol versions 5.0, 3.1.1 and 3.1. Mosquitto is lightweight and is suitable for use on all devices from low power single board computers to full servers. The MQTT protocol provides a lightweight method of carrying out messaging using a publish/subscribe model. This makes it suitable for Internet of Things messaging such as with low power sensors or mobile devices such as phones, embedded computers or microcontrollers.	https://mosquitto.org/	Capability	Red Team Operations	Training and Practice Systems	Victim VM			
MQTT benchmarking tool	MQTT benchmarking tool	Tool	IoT, IIoT	Cloud Infrastructure	A simple MQTT (broker) benchmarking tool.	https://github.com/krylovsk/mqtt-benchmark	Capability	Scenario	Infrastructure	Benchmarking / Load Testing			
5g-trace-visualizer	SVG sequence diagram converter	Tool	RAN & Mobile Devices	5G and 6G Security	This set of Python scripts allow you to convert pcap, pcapng or pdml 5G protocol traces (Wireshark, tcpdump, ...) into SVG sequence diagrams.	https://github.com/telekom/5g-trace-visualizer	Capability	Monitoring and Analytics	Analysis & Verification	Measure the Procedure completion time (PCT)			
CSV	Structured Data Exchange	Data Format	RAN & Mobile Devices	5G and 6G Security	CSV is one of the most popular formats for publishing data on the web. It is concise, easy to understand by both humans and computers, and aligns nicely to the tabular nature of most data.	https://www.w3.org/2013/csvw/wiki/Main_Page.html	Capability	Custom Development	Dataset Generation	Data Format for Network Traffic			
Free5GC	Open-source 5G core network for testing and research	Tool	RAN & Mobile Devices	5G and 6G Security	Open5GS is an advanced, open-source project designed for building and managing your own NR/LTE mobile network.	https://open5gs.org/	Core Technology	Scenario	Infrastructure	5G Core Network Simulation			
free5gc-compose	Container-Orchestrierung	Tool	RAN & Mobile Devices	5G and 6G Security	This repository is a docker compose version of free5GC for stage 3. It's inspired by free5gc-docker-compose and also reference to docker-free5gc.	https://github.com/free5gc/free5gc-compose	Orchestration	Scenario	Create/Edit	Container Orchestration			
OpenStack	Cloud Infrastructure & Management	Tool	RAN & Mobile Devices	5G and 6G Security	OpenStack is a set of software components that provide common services for cloud infrastructure.	https://www.openstack.org/	Core Technology	Computing Platform	Cloud Infrastructure	Dynamic control over the compute, storage, and network resources needed for the digital twin instantiation			
TensorFlow	AI & Machine Learning Application Development	Framework	RAN & Mobile Devices	5G and 6G Security	TensorFlow is an end-to-end platform that makes it easy for you to build and deploy ML models.	https://www.tensorflow.org/	Capability	Custom Development	AI & Machine Learning	Model development and training			
Transformers	Pretrained AI models	Library	RAN & Mobile Devices	5G and 6G Security	Transformers provides APIs and tools to easily download and train state-of-the-art pretrained models. Using pretrained models can reduce your compute costs, carbon footprint, and save you the time and resources required to train a model from scratch. These models support common tasks in different modalities, such as:	https://huggingface.co/docs/transformers/	Capability	Custom Development	AI & Machine Learning	Model development and training			
Tshark	Network Traffic Analysis	Tool	RAN & Mobile Devices	5G and 6G Security	A command-line network protocol analyzer, part of the Wireshark suite.	https://www.wireshark.org/docs/man-pages/tshark.html	Capability	Monitoring and Analytics	Analysis & Verification	Packet capture			
UERANSIM	5G user equipment (UE) and RAN simulator	Tool	RAN & Mobile Devices	5G and 6G Security	Open source state-of-the-art 5G UE and RAN (gNodeB) simulator. UE and RAN can be considered as a 5G mobile phone and a base station in basic terms.	https://github.com/aligungr/UERANSIM	Capability	Scenario	Infrastructure	5G Network Simulation			
Wireshark	Network Traffic Analysis	Tool	RAN & Mobile Devices	5G and 6G Security	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Monitoring and Analytics	Data Collection	Packet capture			
Cyber Kill Chain (CKC)	Model for identification and prevention of cyber intrusions activity	Tool	ICS	Power Systems	Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.	https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html	Capability	Red Team Operations	Attack Strategy & Support	Basis for building specific threat models			
IEC 60870-5-104	Smart Grid Communication	Protocol	ICS	Power Systems	A protocol standard for telecontrol using standard transport profiles, enabling communication between control centers and substations over TCP/IP networks.		Capability	Scenario	Infrastructure	Industrial communication			
IEC61850	Industrial Communication	Protocol	ICS	Power Systems	From its start, the IEC 61850 series encompasses many facets to offer to the market a unique way of building-up multi-manufacturers interoperable solutions, including a structured set of standardized machine level words (data model), possibly handled through a standardized machine processable language (SCL – especially for engineering tools), together with a set of standardized communication services, supported by a limited set of standardized communication protocols.	https://iec61850.dvl.iec.ch/	Capability	Scenario	Infrastructure	Industrial communication			
Metasploit	Penetration testing	Tool	ICS	Power Systems	The world's most used penetration testing framework	https://www.metasploit.com/	Capability	Red Team Operations	Exploitation and Attack Execution	Data manipulation/injection attack in PLC			
MITRE ATT&CK	Knowledge base of adversary tactics and techniques	Tool	ICS	Power Systems	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.	https://attack.mitre.org/	Capability	Red Team Operations	Attack Strategy & Support	Basis for building specific threat models			
MITRE Caldera	Adversary Emulation Platform	Tool	ICS	Power Systems	A Scalable, Automated Adversary Emulation Platform Caldera™ is a cybersecurity framework developed by MITRE that empowers cyber practitioners to save time, money, and energy through automated security assessments.	https://caldera.mitre.org/	Capability	Red Team Operations	Adversary emulation	Vulnerability assessment			



Matlab's 5G toolbox	5G simulation	Tool	RAN & Mobile Devices	Aeronautics/Unmanned aerial vehicles (UAVs)	5G Toolbox provides standard-compliant functions and reference examples for the modeling, simulation, and verification of 5G and 5G-Advanced communications systems.	https://uk.mathworks.com/products/5g.html	Core Technology
MAVLink	UAV Communication	Protocol	RAN & Mobile Devices	Aeronautics/Unmanned aerial vehicles (UAVs)	Lightweight messaging protocol for drones and onboard drone components.	https://mavlink.io/	Core Technology
NSF POWDER Wireless platform	Cyber Range	Technology Stack	RAN & Mobile Devices	Aeronautics/Unmanned aerial vehicles (UAVs)	Powder (the Platform for Open Wireless Data-driven Experimental Research) is flexible infrastructure enabling a wide range of software-defined experiments on the future of wireless networks.	https://powderwireless.net/	Core Technology
srsRAN	Open-source 5G RAN Solution	Tool	RAN & Mobile Devices	Aeronautics/Unmanned aerial vehicles (UAVs)	The srsRAN Project is a complete 5G RAN solution, featuring an ORAN-native CU/DU developed by SRS.	https://www.srslte.com/	Core Technology
ZeroMQ	Concurrency and messaging	Library	RAN & Mobile Devices	Aeronautics/Unmanned aerial vehicles (UAVs)	ZeroMQ (also known as ØMQ, 0MQ, or zmq) looks like an embeddable networking library but acts like a concurrency framework. It gives you sockets that carry atomic messages across various transports like in-process, inter-process, TCP, and multicast.	https://zeromq.org/	Capability
CVSS	Common Vulnerability Scoring System	Tool	ICT	General Purpose	The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.	https://www.first.org/cvss/	Capability
Microsoft CyberBattleSim	Testbed	Tool	ICT	General Purpose	Adversaries show no restraint in adopting tools and techniques that can help them attain their goals. To stay ahead of them, Microsoft continues to harness AI and machine learning to solve security challenges. One area we've been experimenting on is autonomous systems. We examine how autonomous agents interact within a simulated enterprise network, and how reinforcement learning techniques can help improve security. We release the source code of a research toolkit we call CyberBattleSim on GitHub. This experimental research project investigates how autonomous agents operate in a simulated enterprise environment using high-level abstraction of computer networks and cybersecurity concepts. The toolkit uses the Python-based OpenAI Gym interface to train automated agents with reinforcement learning algorithms. The code is available at https://github.com/microsoft/CyberBattleSim(opens in new tab).	https://www.microsoft.com/en-us/research/project/cyberbattlesim/	Core Technology
PfSense	Firewall and routing platform	Tool	ICT	Cloud Infrastructure	Open-source firewall and router platform based on FreeBSD.	https://www.pfsense.org/	Capability
Skytap	Cloud computing services	Platform	ICT	Cloud Infrastructure	Cloud service for running traditional and cloud-native applications. It supports environments like VMware, IBM Power, and more.	https://www.skytap.com/	Core Technology
Splunk	Machine-generated analysis platform	Platform	ICT	Cloud Infrastructure	Platform for collecting, analyzing, and visualizing machine-generated data such as logs, metrics, and application events.	https://www.splunk.com/	Capability
Windows Task Scheduler	Automated task execution based on triggers	Tool	ICT	Cloud Infrastructure	The Task Scheduler enables you to automatically perform routine tasks on a chosen computer. The Task Scheduler does so by monitoring whatever criteria you choose (referred to as triggers) and then executing the tasks when those criteria are met.	https://learn.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page	Capability
Wordpress	CMS for website and blog creation	Tool	ICT	Cloud Infrastructure	Free and open-source content management system (CMS) widely used for creating websites, blogs, and applications.	https://wordpress.org/	Capability
XAMPP	Apache distribution with MariaDB, PHP, and Perl	Technology Stack	ICT	Cloud Infrastructure	XAMPP is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl.	https://www.apachefriends.org/	Capability
gym-pybullet-drones	OpenAI Gym environment	Tool	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	Simple OpenAI Gym environment based on PyBullet for multi-agent reinforcement learning with quadrotors	https://utiasdsl.github.io/gym-pybullet-drones/	Core Technology
Nmap	Network discovery	Tool	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	Nmap ("Network Mapper") is an open source tool for network exploration and security auditing.	https://nmap.org/	Capability
Optuna	Hyperparameter optimization framework	Framework	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	Optuna is an automatic hyperparameter optimization software framework, particularly designed for machine learning. It features an imperative, define-by-run style user API. Thanks to our define-by-run API, the code written with Optuna enjoys high modularity, and the user of Optuna can dynamically construct the search spaces for the hyperparameters.	https://optuna.org/	Capability
PyBullet Physics Engine	Bullet Real-Time Physics Simulation	Library	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	Bullet Physics is a professional open source collision detection, rigid body and soft body dynamics library written in portable C++. The library is primarily designed for use in games, visual effects and robotic simulation. The library is free for commercial use under the ZLib license.	https://pybullet.org/wordpress/	Core Technology
PyTorch	Deep learning library	Library	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	PyTorch is an optimized tensor library for deep learning using GPUs and CPUs.	https://pytorch.org/	Capability
Wireshark	Network Traffic Analysis	Tool	CPS	Aeronautics/Unmanned aerial vehicles (UAVs)	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability
Apache web server	Open-source Web server	Tool	IoT, IIoT	General Purpose	The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.	https://httpd.apache.org/	Capability
Aposemat IoT-23 Dataset	Dataset	Dataset	IoT, IIoT	General Purpose	IoT-23 is a new dataset of network traffic from Internet of Things (IoT) devices. It has 20 malware captures executed in IoT devices, and 3 captures for benign IoT devices traffic. It was first published in January 2020, with captures ranging from 2018 to 2019. This IoT network traffic was captured in the Stratosphere Laboratory, AIC group, FEL, CTU University, Czech Republic. Its goal is to offer a large dataset of real and labeled IoT malware infections and IoT benign traffic for researchers to develop machine learning algorithms. This dataset and its research is funded by Avast Software, Prague.	https://www.stratosphereips.org/datasets-iot23	Capability
CICIOT-2023	Dataset	Dataset	IoT, IIoT	General Purpose	The main goal of this research is to propose a novel and extensive IoT attack dataset to foster the development of security analytics applications in real IoT operations. To accomplish this, 33 attacks are executed in an IoT topology composed of 105 devices. These attacks are classified into seven categories, namely DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai. Finally, all attacks are executed by malicious IoT devices targeting other IoT devices.	https://www.unb.ca/cic/datasets/iotdataset-2023.html	Capability
CSV	Structured Data Exchange	Data Format	IoT, IIoT	General Purpose	CSV is one of the most popular formats for publishing data on the web. It is concise, easy to understand by both humans and computers, and aligns nicely to the tabular nature of most data.	https://www.w3.org/2013/csvw/wiki/Main_Page.html	Capability
DPKT	Packet parsing	Library	IoT, IIoT	General Purpose	dpkt is a python module for fast, simple packet creation / parsing, with definitions for the basic TCP/IP protocols	https://dpkt.readthedocs.io/en/latest/index.html	Capability
Mininet	Network Emulation	Framework	IoT, IIoT	General Purpose	Mininet creates a realistic virtual network, running real kernel, switch and application code, on a single machine (VM, cloud or native), in seconds, with a single command.	https://mininet.org/	Core Technology
P4 BMv2 software switch	Open-source virtual switch	Tool	IoT, IIoT	General Purpose	bmv2 is not meant to be a production-grade software switch. It is meant to be used as a tool for developing, testing and debugging P4 data planes and control plane software written for them.	https://github.com/p4lang/behavioral-model	Capability
P4Utils	Mininet Extension	Tool	IoT, IIoT	General Purpose	P4-Utils is an extension to Mininet that makes P4 networks easier to build, run and debug. P4-utils is strongly inspired by p4app. Here we only provide a quick summary of the main information about P4-Utils. Check out the online documentation for more details about P4-Utils installation and usage.	https://github.com/nsg-ethz/p4-utils	Capability
Pandas	Data analysis and manipulation	Library	IoT, IIoT	General Purpose	Pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language.	https://pandas.pydata.org/	Capability
scapy	Python packet manipulation	Tool	IoT, IIoT	General Purpose	Scapy is a powerful interactive packet manipulation library written in Python.	https://scapy.net/	Capability
Slowloris	Denial of Service attack	Tool	IoT, IIoT	General Purpose	Slowloris is basically an HTTP Denial of Service attack that affects threaded servers.	https://github.com/gkbrk/slowloris	Capability
Tcpreplay	Replay captured network traffic	Tool	IoT, IIoT	General Purpose	Tcpreplay is a suite of free Open Source utilities for editing and replaying previously captured network traffic. Originally designed to replay malicious traffic patterns to Intrusion Detection/Prevention Systems, it has seen many evolutions including capabilities to replay to web servers.	https://tcpreplay.appneta.com/	Capability
CyRIS	Cyber Range	Technology Stack	ICT	General Purpose	CyRIS is a tool for facilitating cybersecurity training by automating the creation and management of the corresponding training environments (a.k.a., cyber ranges) based on a description in YAML format. CyRIS is being developed by the Cyber Range Organization and Design (CROND) NEC-endowed chair at the Japan Advanced Institute of Science and Technology (JAIST).	https://github.com/crond-jaist/cyris	Orchestration
Iptables/Nftables	Linux firewall and packet filtering	Tool	ICT	General Purpose	Iptables is the userspace command line program used to configure the Linux 2.4.x and later packet filtering ruleset. It is targeted towards system administrators.	https://www.netfilter.org/projects/iptables/	Core Technology
KVM	Virtualization Platform	Tool	ICT	General Purpose	KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.	https://linux-kvm.org/page/Main_Page	Core Technology
Metasploit	Penetration testing	Tool	ICT	General Purpose	The world's most used penetration testing framework	https://www.metasploit.com/	Capability
Nmap	Network discovery	Tool	ICT	General Purpose	Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.	https://nmap.org/	Capability
pymetasploit3	Python API for Metasploit RPC	Library	ICT	General Purpose	PyMetasploit is a full-fledged msfrpc library for Python. It is meant to interact with the msfrpcd daemon that comes with the latest versions of Metasploit.	https://github.com/allfro/pymetasploit	Capability
python-nmap	Automated Nmap Scanning	Library	ICT	General Purpose	python-nmap is a python library which helps in using nmap port scanner. It allows to easilly manipulate nmap scan results and will be a perfect tool for systems administrators who want to automatize scanning task and reports. It also supports nmap script outputs.	https://pypi.org/project/python-nmap/	Capability
YAML	Data serialization language	Data Format	ICT	General Purpose	YAML is a human-friendly data serialization language for all programming languages.	https://yaml.org/	Orchestration
Apache JMeter	Testing Web Applications	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	The Apache JMeter™ application is open source software, a 100% pure Java application designed to load test functional behavior and measure performance. It was originally designed for testing Web Applications but has since expanded to other test functions.	https://jmeter.apache.org/	Capability
cpprestsdk	Connect to and interact with services	Library	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	The C++ REST SDK is a Microsoft project for cloud-based client-server communication in native code using a modern asynchronous C++ API design. This project aims to help C++ developers connect to and interact with services.	https://github.com/microsoft/cpprestsdk	Capability
Docker	Containerisation technology	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Docker Engine is an open source Containerisation technology for building and containerizing your applications.	https://www.docker.com/	Core Technology
Hyperledger Composer	Application development framework	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Hyperledger Composer is an application development framework which simplifies and expedites the creation of Hyperledger fabric blockchain applications.	https://hyperledger.github.io/composer/latest/	Capability
Hyperledger Fabric	Distributed ledger technology (DLT) platform	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Hyperledger Fabric is an open source enterprise-grade permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms.	https://hyperledger-fabric.readthedocs.io/en/release-2.5/	Capability
Node.js	JavaScript runtime environment	Framework	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Node.js® is a free, open-source, cross-platform JavaScript runtime environment that lets developers create servers, web apps, command line tools and scripts.	https://nodejs.org/	Capability
ProVerif	Cryptographic protocol verifier	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	ProVerif is an automatic cryptographic protocol verifier, in the formal model (so called Dolev-Yao model). This protocol verifier is based on a representation of the protocol by Horn clauses.	https://bblanche.gitlabpages.inria.fr/proverif/	Capability
SUMO	Urban mobility and traffic simulation	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Simulation of Urban MObility" (SUMO) is an open source, highly portable, microscopic and continuous traffic simulation package designed to handle large networks.	https://sumo.dlr.de/docs/index.html	Core Technology
VENTOS	Network simulation framework based on OMNeT++ and SUMO	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)	Features VENTOS is an integrated C++ simulator for studying vehicular traffic flows, collaborative driving, and interactions between vehicles and infrastructure through DSRC-enabled wireless communication capability. It is the main tool in C3PO project. Here are some of the features that we think that you'll love:	https://maniam.github.io/VENTOS/#about	Core Technology
Ansible	Orchestration & Configuration Management	Tool	ICT	General Purpose	Ansible is an open source IT automation engine that automates provisioning, configuration management, application deployment, orchestration, and many other IT processes. IaC	https://www.ansible.com/	Orchestration
ELK Stack	Data collection and analytics platform	Technology Stack	ICT	General Purpose	It's comprised of Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack) and more. Reliably and securely take data from any source, in any format, then search, analyze, and visualize.	https://www.elastic.co/	Capability
Hydra	Brute-force password-cracking	Tool	ICT	General Purpose	Fast and flexible password-cracking tool designed to perform brute-force attacks against various protocols and services.	https://github.com/vanhauser-thc/thc-hydra	Capability
John The Ripper	Password security auditing and recovery	Tool	ICT	General Purpose	John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems.	https://www.openwall.com/john/	Capability
Kibana	Systems monitoring and alerting	Tool	ICT	General Purpose	An data analytics at speed and scale for observability, security, and search with Kibana. Powerful analysis on any data from any source, from threat intelligence to search analytics, logs to application monitoring, and much more.	https://www.elastic.co/kibana	Capability
LinPEAS	Privilege Escalation	Tool	ICT	General Purpose	These tools search for possible local privilege escalation paths that you could exploit and print them to you with nice colors so you can recognize the misconfigurations easily.	https://github.com/peass-ng/PEASS-ng	Capability
Moodle	Online learning management system	Tool	ICT	General Purpose	Moodle is a free, online Learning Management system enabling educators to create their own private website filled with dynamic courses that extend learning, any time, anywhere.	https://moodle.org/	Capability
OpenSSH	Secure remote login	Tool	ICT	General Purpose	OpenSSH is the premier connectivity tool for remote login with the SSH protocol.	https://www.openssh.com/	Capability
Packer	Automated image creation	Tool	ICT	General Purpose	Create identical images for multiple platforms from a single source configuration.	https://www.packer.io/	Orchestration
ProM	Process mining	Tool	ICT	General Purpose	ProM is an extensible framework that supports a wide variety of process mining techniques in the form of plug-ins. It is platform independent as it is implemented in Java, and can be downloaded free of charge.		Capability
Terraform	Infrastructure as Code (IaC)	Tool	ICT	General Purpose	Software Orchestration & Configuration to provision and manage resources in any cloud or data center, IaC	https://www.terraform.io/	Orchestration
Windows Remote desktop protocol (RDP)	Remote desktop access	Tool	ICT	General Purpose	Proprietary protocol for accessing and managing remote desktops	https://www.microsoft.com	Capability
Controller Area Network (CAN)	High-integrity serial bus system	Protocol	Intelligent Transportation Systems	In-vehicle networks	A controller area network (CAN) bus is a high-integrity serial bus system for networking intelligent devices. CAN busses and devices are common components in automotive and industrial systems.	https://www.bosch-semiconductors.com/products/ip-modules/can-protocols/	Capability
MQTT	IoT Messaging protocol	Protocol	Intelligent Transportation Systems	In-vehicle networks	Lightweight messaging protocol for IoT communication.	https://mqtt.org/	Capability
OpenTAP	Test automation	Tool	Intelligent Transportation Systems	In-vehicle networks	The core of OpenTAP is a cross-platform and open source test sequencer for hardware and software test automation — constantly strengthening as our community adds plugins and contributors.	https://opentap.io/	Orchestration
PASTA (Portable Automotive Security Testbed with Adaptability)	Testbed	Technology Stack	Intelligent Transportation Systems	In-vehicle networks	PASTA:Portable Automotive Security Testbed with Adaptability, developed by Toyota InfoTechnology Center, is a platform based on non-proprietary technology, allowing researchers or engineers to freely construct in-vehicle networks. PASTA will contribute to accelerate research, education, and information sharing of vehicle cybersecurity as an open and handy platform which has typical physical attack surfaces.	https://github.com/pasta-auto/PASTA1.0	Core Technology
Unity3D	Game Development and Simulation	Tool	Intelligent Transportation Systems	In-vehicle networks	Unity's industry-leading engine provides tools to create and run amazing games and other real-time interactive experiences and publish to a variety of devices.	https://unity.com/	Core Technology
MATLAB/Simulink	Cyber-physical system simulation	Tool	Power Systems	Cyber-Physical Power Systems	Simulink Desktop Real-Time provides a real-time kernel for Windows, Linux, and macOS. It includes drag-and-drop Simulink I/O driver blocks that enable closed-loop control of physical systems from your desktop computer. The toolbox lets you connect to sensors, actuators, and other devices to prototype and test control systems without requiring dedicated real-time test equipmen	https://www.mathworks.com/products/simulink-desktop-real-time.html	Core Technology
OPNET	Network performance simulation	Tool	Power Systems	Cyber-Physical Power Systems	OPNET Network simulator is a tool to simulate the behavior and performance of any type of network. The main difference Opnet Network Simulator comparing to other simulators lies in its power and versatility.	https://opnetprojects.com/opnet-network-simulator/	Core Technology
RT-LAB	Real-time simulation for power systems integrated with MATLAB/Simulink	Tool	Power Systems	Cyber-Physical Power Systems	Fully integrated with MATLAB/Simulink, RT-LAB enables Simulink models to interact with the real world in real-time. This makes RT-LAB an ideal software platform of real-time simulation for engineers to rapidly develop and validate their applications, regardless of their complexity. As a multi-domain platform, RT-LAB provides flexible and scalable solutions for the power systems, power electronics, aerospace, and automotive industries.	https://www.opal-rt.com/software-rt-lab/	Core Technology
Amazon Web Services (AWS)	Cloud computing services	Platform	CPS	Residential Energy Storage Systems (RESSs)	Amazon Web Services (AWS) is the world's most comprehensive and widely used cloud, with more than 200 services offering extensive functionality and delivered from globally distributed data centers.	https://aws.amazon.com/	Core Technology
JSON	Structured Data Exchange	Data Format	CPS	Residential Energy Storage Systems (RESSs)	JSON (JavaScript Object Notation) is a lightweight Structured Data Exchange format.	https://www.json.org/json-en.html	Capability
MATLAB/Simulink	Cyber-physical system simulation	Tool	CPS	Residential Energy Storage Systems (RESSs)	Simulink Desktop Real-Time provides a real-time kernel for Windows, Linux, and macOS. It includes drag-and-drop Simulink I/O driver blocks that enable closed-loop control of physical systems from your desktop computer. The toolbox lets you connect to sensors, actuators, and other devices to prototype and test control systems without requiring dedicated real-time test equipmen	https://www.mathworks.com/products/simulink-desktop-real-time.html	Core Technology
Modbus	Communication protocol for industrial devices	Protocol	CPS	Residential Energy Storage Systems (RESSs)	It is used to establish client-server communication between intelligent devices. It is a de facto standard, truly open and the most widely used network protocol in the industrial manufacturing environment.	https://modbus.org/	Capability
MQTT	IoT Messaging protocol	Protocol	CPS	Residential Energy Storage Systems (RESSs)	Lightweight messaging protocol for IoT communication.	https://mqtt.org/	Capability
Node-RED	Flow-based programming	Tool	CPS	Residential Energy Storage Systems (RESSs)	Node-RED is a programming tool for wiring together hardware devices, APIs and online services in new and interesting ways.	https://nodered.org/	Capability
DNP3	Electric transmission and industrial communication	Protocol	ICS	General Purpose	DNP3 has grown to be the most widely used protocol for electric transmission and distribution communications in North America and other regions of the world, and is a named standard for DER communications. DNP3 is also broadly adopted in adjacent industries such as water / wastewater, transportation and the oil and gas industry.	https://www.dnp.org/	Core Technology
GRFICS	Graphical Framework for ICS	Technology Stack	ICS	General Purpose	This version of GRFICS is organized as 5 VirtualBox VMs (a 3D simulation, a soft PLC, an HMI, a pfsense firewall, and a workstation) communicating with each other on host-only virtual networks.	https://github.com/Fortiphyd/GRFICSv2	Capability
Ignition SCADA	SCADA System	Tool	ICS	General Purpose	Ignition SCADA by Inductive Automation® combines an unlimited licensing model, with instant web-based deployment, and the industry-leading toolset for supervisory control and data acquisition (SCADA) — all on one open and scalable universal platform. Ignition is The New SCADA because it solves all the major pain points of old SCADA .	https://inductiveautomation.com/scada-software/	Capability
Modbus	Communication protocol for industrial devices	Protocol	ICS	General Purpose	It is used to establish client-server communication between intelligent devices. It is a de facto standard, truly open and the most widely used network protocol in the industrial manufacturing environment.	https://modbus.org/	Capability
NETLAB+	Remote access solution	Tool	ICS	General Purpose	Deliver world-class content in the latest IT technologies to students all over the world. NETLAB+ is a remote access solution that lets students complete labs anywhere, and anytime. So you're able to serve more students, expand your curriculum, and maximize the utilization of your valuable IT infrastructure.	https://www.netdevgroup.com/products/	Capability
OPC Unified Architecture (OPC-UA)	Communication protocol for industrial devices	Protocol	ICS	General Purpose	The OPC Unified Architecture (UA), released in 2008, is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework.	https://opcfoundation.org/about/opc-technologies/opc-ua/	Capability
OpenPLC	Open-source programmable logic controller	Tool	ICS	General Purpose	OpenPLC is an open-source Programmable Logic Controller that is based on an easy to use software. It is the first fully functional standardized open source PLC, both in software and in hardware.	https://www.openplcproject.com/	Capability
Typhoon-HIL	Hardware-in-the-Loop (HIL) solution	Tool	ICS	General Purpose	Typhoon HIL602+ is an ideal all-around tool for development, automated testing, optimization, and automated standardized pre-certification of grid connected converters, automotive converters, electric propulsion drives for terrestrial and marine vehicles, and smaller microgrids.	https://www.typhoon-hil.com/	Core Technology
VMWare ESXi	Virtualization Platform	Tool	ICS	General Purpose	The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.	https://www.vmware.com/products/cloud-infrastructure/vsphere	Core Technology
ANSYS	Multiphysics simulation for engineering applications	Tool	Intelligent Transportation Systems	Electric Vehicle Powertrain	Ansys offers a comprehensive software suite that spans the entire range of physics, providing access to virtually any field of Engineering simulations that a design process requires.	https://www.ansys.com/	Core Technology
MATLAB/Simulink	Cyber-physical system simulation	Tool	Intelligent Transportation Systems	Electric Vehicle Powertrain	Simulink Desktop Real-Time provides a real-time kernel for Windows, Linux, and macOS. It includes drag-and-drop Simulink I/O driver blocks that enable closed-loop control of physical systems from your desktop computer. The toolbox lets you connect to sensors, actuators, and other devices to prototype and test control systems without requiring dedicated real-time test equipmen	https://www.mathworks.com/products/simulink-desktop-real-time.html	Core Technology
Opal-RT Simulator	Real-time simulation for power systems and hardware-in-the-loop (HIL)	Tool	Intelligent Transportation Systems	Electric Vehicle Powertrain	Real-time simulation platform for power systems and hardware-in-the-loop testing.	https://www.opal-rt.com/	Core Technology
Docker	Containerisation technology	Tool	ICT	General Purpose	Docker Engine is an open source Containerisation technology for building and containerizing your applications.	https://www.docker.com/	Core Technology

Hping	TCP/IP packet generator	Tool	IoT, IIoT	IoT, IIoT Communication Security
MQTT	IoT Messaging protocol	Protocol	IoT, IIoT	IoT, IIoT Communication Security
Node-RED	Flow-based programming	Tool	IoT, IIoT	IoT, IIoT Communication Security
Wireshark	Network Traffic Analysis	Tool	IoT, IIoT	IoT, IIoT Communication Security
ARINC 653 software emulator	ARINC653 kernel simulator	Tool	CPS	Autonomous Vehicle Security
Binary Ninja	Software Analysis & Reverse Engineering	Tool	CPS	Autonomous Vehicle Security
CARLA	Open-source autonomous driving simulator	Tool	CPS	Autonomous Vehicle Security
CUDA	GPU computing platform	Tool	CPS	Autonomous Vehicle Security
Mambo	Binary instrumentation	Tool	CPS	Autonomous Vehicle Security
Mcsema	Software Analysis & Reverse Engineering	Framework	CPS	Autonomous Vehicle Security
SVF library	Static Program Analysis Tool	Library	CPS	Autonomous Vehicle Security
TensorFlow	AI & Machine Learning Application Development	Framework	CPS	Autonomous Vehicle Security
Tensorflow Lite	AI & Machine Learning Application Development	Library	CPS	Autonomous Vehicle Security
ZeroMQ	Concurrency and messaging	Library	CPS	Autonomous Vehicle Security
Ansible	Orchestration & Configuration Management	Tool	Power Systems	Smart Grid
Arpspoof	ARP cache poisoning	Tool	Power Systems	Smart Grid
DLMS/COSEM	Smart energy metering and control	Protocol	Power Systems	Smart Grid
GIT	Version Control System	Tool	Power Systems	Smart Grid
Gurux	Industrial device communication	Tool	Power Systems	Smart Grid
OpenStack	Cloud Infrastructure & Management	Tool	Power Systems	Smart Grid
Tcpdump	Command-line packet analyzer	Tool	Power Systems	Smart Grid
YAML	Data serialization language	Data Format	Power Systems	Smart Grid
Ansible	Orchestration & Configuration Management	Tool	ICT	General Purpose
Apache web server	Open-source Web server	Tool	ICT	General Purpose
Contrast Security	Security platform for applications and APIs	Tool	ICT	General Purpose
Docker	Containerisation technology	Tool	ICT	General Purpose
DVWA	Vulnerable web application	Tool	ICT	General Purpose
GNS3	Network emulation	Tool	ICT	General Purpose
Infection Monkey	Adversary emulation	Tool	ICT	General Purpose
Metasploit	Penetration testing	Tool	ICT	General Purpose
Nessus	Vulnerability Scanner	Tool	ICT	General Purpose
Nikto	Web Application Scanner	Tool	ICT	General Purpose
Nmap	Network discovery	Tool	ICT	General Purpose
Owasp WebGoat	Vulnerable web application	Tool	ICT	General Purpose
Owasp Zap (Zed Attack Proxy)	Web Application Scanner	Tool	ICT	General Purpose
VMWare vSphere	Virtualization platform	Tool	ICT	General Purpose
Wordpress	CMS for website and blog creation	Tool	ICT	General Purpose
Free5GC	Open-source 5G core network for testing and research	Tool	RAN & Mobile Devices	5G and 6G Security
MANO	Management and orchestration for NFV	Tool	RAN & Mobile Devices	5G and 6G Security
ONOS	Open-source SDN controller	Tool	RAN & Mobile Devices	5G and 6G Security
OpenFlow	Software-Defined Networking (SDN)	Protocol	RAN & Mobile Devices	5G and 6G Security
OpenStack	Cloud Infrastructure & Management	Tool	RAN & Mobile Devices	5G and 6G Security
scapy	Python packet manipulation	Library	RAN & Mobile Devices	5G and 6G Security
sFlow	High-speed network monitoring	Tool	RAN & Mobile Devices	5G and 6G Security
URLhaus	Malicious URL Database	Tool	RAN & Mobile Devices	5G and 6G Security
YAML	Data serialization language	Data Format	RAN & Mobile Devices	5G and 6G Security
Zeek	Network security monitoring and traffic analysis	Tool	RAN & Mobile Devices	5G and 6G Security
Gephi	Visualization and exploration software	Tool	ICT	Supercomputing
osquery	OS monitoring with SQL queries	Tool	ICT	Supercomputing
OSSEC	Host-based Intrusion Detection System (HIDS)	Tool	ICT	Supercomputing
PostgreSQL	Relational database	Tool	ICT	Supercomputing
QEMU	Machine emulator and virtualizer	Tool	ICT	Supercomputing
rsyslog	Logging Framework	Tool	ICS	Supercomputing
Vulnerability Reproduction Tool (VRT)	Automated image creation	Tool	ICT	Supercomputing
Zeek	Network security monitoring and traffic analysis	Tool	ICT	Supercomputing
curl-loader	Simulating application load	Tool	ICT	Cloud Infrastructure
Hping	TCP/IP packet generator	Tool	ICT	Cloud Infrastructure
Keras	Deep learning API built on TensorFlow, JAX, or PyTorch	Library	ICT	Cloud Infrastructure
Matplotlib	Data visualization	Library	ICT	Cloud Infrastructure
Mininet	Network Emulation	Framework	ICT	Cloud Infrastructure
NetworkX	Network Analysis	Library	ICT	Cloud Infrastructure
NumPy	Scientific computing	Library	ICT	Cloud Infrastructure
OpenFlow	Software-Defined Networking (SDN)	Protocol	ICT	Cloud Infrastructure
Pandas	Data analysis and manipulation	Library	ICT	Cloud Infrastructure
Ryu	Component-based software defined networking framework	Tool	ICT	Cloud Infrastructure
Seaborn	Data visualization	Library	ICT	Cloud Infrastructure
Tcpdump	Command-line packet analyzer	Tool	ICT	Cloud Infrastructure
TensorFlow	AI & Machine Learning Application Development	Framework	ICT	Cloud Infrastructure
Tshark	Network Traffic Analysis	Tool	ICT	Cloud Infrastructure
MITRE ATT&CK	ATT&CK knowledge base	Tool	ICT	General Purpose
MITRE Caldera	Adversary Emulation Platform	Tool	ICT	General Purpose
MulVAL	Vulnerability analysis	Tool	ICT	General Purpose
Suricata	Intrusion Detection and Prevention System (IDS/IPS)	Tool	ICT	General Purpose
Wazuh SIEM	Unified XDR and SIEM protection	Tool	ICT	General Purpose
Windows Active Directory	Centralized authentication and authorization system	Platform	ICT	General Purpose
IEC 60870-5-104	Smart Grid Communication	Protocol	Power Systems	Power Grid
IPAL Toolset	Industrial Protocol Abstraction Layer	Tool	Power Systems	Power Grid
PowerOwl	Power grid architecture modeling	Tool	Power Systems	Power Grid
Simbench	Data set and benchmark for the simulation of power grids	Data set	Power Systems	Power Grid
Wattson	Research testbed	Technology Stack	Power Systems	Power Grid
Cyber Physical Systems Wind Tunnel (CPSWT)	Cyber-Physical System simulation	Tool	CPS	Railway Systems
Grafana	Systems monitoring and alerting	Tool	CPS	Railway Systems
InfluxDB	Time-series database	Tool	CPS	Railway Systems
OMNeT++	Network Emulation	Tool	CPS	Railway Systems
SocketCAN	Linux-based CAN protocol implementation	Protocol	CPS	Railway Systems
SUMO	Urban mobility and traffic simulation	Tool	CPS	Railway Systems
V2X	Vehicle-to-everything communication	Protocol	CPS	Railway Systems

Veins	Vehicular network simulation	Tool	CPS	Railway Systems
WebGME	Web-based collaborative modeling tool	Tool	CPS	Railway Systems
ZeroMQ	Concurrency and messaging	Library	CPS	Railway Systems
ABB Robot Studio	ABB robot programming	Tool	ICS	Manufacturing Systems
COMAU PickApp HMI	Robot control interface	Tool	ICS	Manufacturing Systems
KukaSim	KUKA robot programming	Tool	ICS	Manufacturing Systems
Modbus	Communication protocol for industrial devices	Protocol	ICS	Manufacturing Systems
S7comm	Siemens proprietary PLC communication protocol	Protocol	ICS	Manufacturing Systems
Anaconda	Development environment	Framework	ICT	General Purpose
Apache Spark	Unified analytics engine	Tool	ICT	General Purpose
CICFlowMeter	Generates and analyzes network traffic	Tool	ICT	General Purpose
CSV	Structured Data Exchange	Data Format	ICT	General Purpose
Jupyter notebook	Interactive computational notebook	Tool	ICT	General Purpose
NumPy	Scientific computing	Library	ICT	General Purpose
Wireshark	Network Traffic Analysis	Tool	ICT	General Purpose
XAMPP	Apache distribution with MariaDB, PHP, and Perl	Technology Stack	ICT	General Purpose
GOOSE	Publisher-subscriber model for substation communication	Protocol	Power Systems	Manufacturing Systems
MMS	Client-server-based communication in substations	Protocol	Power Systems	Manufacturing Systems
Pandapower	Power system network calculation	Library	Power Systems	Manufacturing Systems
Docker	Containerisation technology	Tool	ICT	Web Applications
Docker Hub	Docker Container Image Library	Tool	ICT	Web Applications
Docker Swarm	Cluster management for Docker	Tool	ICT	Web Applications
DVWA	Vulnerable web application	Tool	ICT	Web Applications
Amazon Web Services (AWS)	Cloud computing services	Platform	ICT	General Purpose
Ansible	Orchestration & Configuration Management	Tool	ICT	General Purpose
Elastic Agent	Collect all forms of data	Tool	ICT	General Purpose
Elastic Security (SIEM)	Security Platform	Platform	ICT	General Purpose
JSON	Structured Data Exchange	Data Format	ICT	General Purpose
Kibana	Systems monitoring and alerting	Tool	ICT	General Purpose
Libvirt	Virtualization Platform management	Tool	ICT	General Purpose
MITRE ATT&CK	Knowledge base of adversary tactics and techniques	Tool	ICT	General Purpose
MITRE Caldera	Adversary Emulation Platform	Tool	ICT	General Purpose
Moodle	Online learning management system	Tool	ICT	General Purpose
OpenSSH	Secure remote login	Tool	ICT	General Purpose
Packer	Automated image creation	Tool	ICT	General Purpose
Packetbeat	Network packet analyzer	Tool	ICT	General Purpose
Terraform	Infrastructure as Code (IaC)	Tool	ICT	General Purpose
Windows Remote desktop protocol (RDP)	Remote desktop access	Tool	ICT	General Purpose
YAML	Data serialization language	Data Format	ICT	General Purpose
Elasticsearch	Data store and search engine	Tool	ICT	General Purpose
Endgame	Endpoint security and extended detection and response (XDR)	Tool	ICT	General Purpose
Jira	Issue and Task Tracking	Tool	ICT	General Purpose
Kibana	Systems monitoring and alerting	Tool	ICT	General Purpose
Nessus	Vulnerability Scanner	Tool	ICT	General Purpose
Suricata	Intrusion Detection and Prevention System (IDS/IPS)	Tool	ICT	General Purpose
ThreatGrid	Malware Analysis	Tool	ICT	General Purpose
VirusTotal	Malware Analysis	Tool	ICT	General Purpose
Windows Active Directory	Centralized authentication and authorization system	Platform	ICT	General Purpose
Metasploit	Penetration testing	Tool	Power Systems	Micro Grid
Mimikatz	Credential extraction	Tool	Power Systems	Micro Grid
MMS	Client-server-based communication in substations	Protocol	Power Systems	Micro Grid
Modbus	Communication protocol for industrial devices	Protocol	Power Systems	Micro Grid
scapy	Python packet manipulation	Tool	Power Systems	Micro Grid
Windows Remote desktop protocol (RDP)	Remote desktop access	Tool	Power Systems	Micro Grid
CSV	Structured Data Exchange	Data Format	IoT, IIoT	Smart Airport
JSON	Structured Data Exchange	Data Format	IoT, IIoT	Smart Airport
LoRa	Low Power Wide Area Network (LPWAN) protocol	Protocol	IoT, IIoT	Smart Airport
Metasploit	Penetration testing	Tool	IoT, IIoT	Smart Airport
Metasploitable	Vulnerable VM	Tool	IoT, IIoT	Smart Airport
MQTT	IoT Messaging protocol	Protocol	IoT, IIoT	Smart Airport
MySQL Database	Relational database	Tool	IoT, IIoT	Smart Airport
Nmap	Network discovery	Tool	IoT, IIoT	Smart Airport
Node-RED	Flow-based programming	Tool	IoT, IIoT	Smart Airport
OSSIM Alien Vault	SIEM platform	Tool	IoT, IIoT	Smart Airport
PfSense	Firewall and routing platform	Tool	IoT, IIoT	Smart Airport
scapy	Python packet manipulation	Tool	IoT, IIoT	Smart Airport
Security Onion	Threat Detection & Security Monitoring	Platform	IoT, IIoT	Smart Airport
sFuzz	Black-box fuzzing	Tool	IoT, IIoT	Smart Airport
Tcpdump	Command-line packet analyzer	Tool	IoT, IIoT	Smart Airport
Thingsboard	Device management, data collection, and visualization	Tool	IoT, IIoT	Smart Airport
Zeek	Network security monitoring and traffic analysis	Tool	IoT, IIoT	Smart Airport
ZigBee	Low-power mesh networking	Protocol	IoT, IIoT	Smart Airport
ZigBee2MQTT	Bridge for ZigBee and MQTT	Protocol	IoT, IIoT	Smart Airport
Z-Wave	Wireless communication protocol for smart homes	Protocol	IoT, IIoT	Smart Airport
Modbus	Communication protocol for industrial devices	Protocol	ICS	Water Reservoir
Nmap	Network discovery	Tool	ICS	Water Reservoir
PsTools	Windows system management	Tool	ICS	Water Reservoir
Wireshark	Network Traffic Analysis	Tool	ICS	Water Reservoir
Ansible	Orchestration & Configuration Management	Tool	ICT	General Purpose
Nmap	Network discovery	Tool	ICT	General Purpose
OPNSense	Firewall and routing platform	Tool	ICT	General Purpose
Pm4py	Process mining	Library	ICT	General Purpose
ProM	Process mining	Tool	ICT	General Purpose
Proxmox VE	Virtualization Platform	Tool	ICT	General Purpose
Terraform	Infrastructure as Code (IaC)	Tool	ICT	General Purpose
Tracee	Threat detection engine	Tool	ICT	General Purpose
Vector	Observability pipeline	Tool	ICT	General Purpose

Acunetix	Automated vulnerability scanning	Tool	ICS	SCADA Security
Arachni	Evaluate the security of web applications.	Tool	ICS	SCADA Security
DESLib (Dynamic Ensemble Selection Library)	Dynamic classifier and ensemble selection	Library	ICS	SCADA Security
FlowTBag	Calculate flow statistics	Tool	ICS	SCADA Security
Honeyd	Simulates thousands of virtual hosts	Tool	ICS	SCADA Security
Iptables/Nftables	Linux firewall and packet filtering	Tool	ICS	SCADA Security
Nessus	Vulnerability Scanner	Tool	ICS	SCADA Security
Nmap	Network discovery	Tool	ICS	SCADA Security
NumPy	Scientific computing	Library	ICS	SCADA Security
Pandas	Data analysis and manipulation	Library	ICS	SCADA Security
ScadaBR	Open-source SCADA system	Tool	ICS	SCADA Security
scapy	Python packet manipulation	Library	ICS	SCADA Security
Smod	Modbus diagnostic	Tool	ICS	SCADA Security
Snort	Intrusion Detection and Prevention System (IDS/IPS)	Tool	ICS	SCADA Security
OMNeT++	Network Emulation	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)
SUMO	Urban mobility and traffic simulation	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)
Veins	Vehicular network simulation	Tool	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)
WAVE protocol	Wireless communication	Protocol	Intelligent Transportation Systems	Vehicular Ad-hoc Networks (VANETs)
INET	Network Simulator	Tool	ICT	General Purpose
NETA	NETwork Attacks Framework for OMNeT++	Tool	ICT	General Purpose
OMNeT++	Network Emulation	Tool	ICT	General Purpose
Ponder2	Policy Framework	Tool	ICT	General Purpose
PReSET	Policy-driven Resilience Strategy Evaluation Toolset	Tool	ICT	General Purpose
ReaSE	Simulation Environments for IP-based Networks	Tool	ICT	General Purpose
SEA++	Simulating Security Attacks	Tool	ICT	General Purpose
Tribe Flood Network (TFN)	DDoS attacks	Tool	ICT	General Purpose
VirtualBox	Virtualization Platform	Tool	ICT	General Purpose
GOOSE	Publisher-subscriber model for substation communication	Protocol	Power Systems	Smart Grid
JSON	Structured Data Exchange	Data Format	Power Systems	Smart Grid
Mininet	Network Emulation	Framework	Power Systems	Smart Grid
MMS	Client-server-based communication in substations	Protocol	Power Systems	Smart Grid
MySQL Database	Relational database	Tool	Power Systems	Smart Grid
OpenPLC	Open-source programmable logic controller	Tool	Power Systems	Smart Grid
Pandapower	Power system network calculation	Library	Power Systems	Smart Grid
R-GOOSE	IP-based extension of GOOSE for wide-area networks	Protocol	Power Systems	Smart Grid
R-SV (Routable Sampled Value)	WAN routing for IEC 61850 Sampled Values	Protocol	Power Systems	Smart Grid
ScadaBR	Open-source SCADA system	Tool	Power Systems	Smart Grid
XML	Structured Data Exchange	Data Format	Power Systems	Smart Grid
Docker	Containerisation technology	Tool	ICS	General Purpose
Dsiem	Security event correlation for ELK Stack	Tool	ICS	General Purpose
ELK Stack	Data collection and analytics platform	Technology Stack	ICS	General Purpose
Ettercap	Man in the middle attacks	Tool	ICS	General Purpose
Kibana	Systems monitoring and alerting	Tool	ICS	General Purpose
MiniCPS	Cyber-Physical Co-Simulation	Tool	ICS	General Purpose
Mininet	Network Emulation	Tool	ICS	General Purpose
scapy	Python packet manipulation	Library	ICS	General Purpose
arp-scan	Host discovery and fingerprinting	Tool	ICT	General Purpose
CSV	Structured Data Exchange	Data Format	ICT	General Purpose
Datalog	Declarative logic programming language	Programming language	ICT	General Purpose
Metasploit	Penetration testing	Tool	ICT	General Purpose
Mimikatz	Credential extraction	Tool	ICT	General Purpose
nbtscan	NetBIOS Network Scanner	Tool	ICT	General Purpose
Netdiscover	ARP scanning	Tool	ICT	General Purpose
Nmap	Network discovery	Tool	ICT	General Purpose
Norwegian Cyber Range	Cyber Range	Tool	ICT	General Purpose
PyDatalog	Python logic programming	Library	ICT	General Purpose
VNCDtool	Command-line VNC client	Tool	ICT	General Purpose
KVM	Virtualization Platform	Tool	ICS	General Purpose
NS3	Discrete-event network simulator	Tool	ICS	General Purpose
OpenStack	Cloud Infrastructure & Management	Tool	ICS	General Purpose
Docker	Containerisation technology	Tool	ICS	Manufacturing Systems
ICSFlowGenerator	Processing of network packets	Tool	ICS	Manufacturing Systems
ICSSIM Framework	Simulating industrial control system	Technology Stack	ICS	Manufacturing Systems
JSON	Structured Data Exchange	Data Format	ICS	Manufacturing Systems
Modbus	Communication protocol for industrial devices	Protocol	ICS	Manufacturing Systems
MQTT Broker	MQTT broker	Tool	ICS	Manufacturing Systems
OMNeT++	Network Emulation	Tool	Intelligent Transportation Systems	Vehicle-To-Everything (V2X) communications
Security Credential Management System (SCMS)	Message security for V2X	Tool	Intelligent Transportation Systems	Vehicle-To-Everything (V2X) communications
SUMO	Urban mobility and traffic simulation	Tool	Intelligent Transportation Systems	Vehicle-To-Everything (V2X) communications
V2X	Vehicle-to-everything communication	Protocol	Intelligent Transportation Systems	Vehicle-To-Everything (V2X) communications
VENTOS	Network simulation framework based on OMNeT++ and SUMO	Tool	Intelligent Transportation Systems	Vehicle-To-Everything (V2X) communications
Minimega	Virtual machine management and deployment	Tool	ICT	General Purpose
Nmap	Network discovery	Tool	ICT	General Purpose
SCORCH	Automated scenario orchestration framework	Tool	ICT	General Purpose
Snort	Intrusion Detection and Prevention System (IDS/IPS)	Tool	ICT	General Purpose
INET	Network Simulator	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
OMNeT++	Network Emulation	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
Scyther	Automatic verification of security protocols	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
SUMO	Urban mobility and traffic simulation	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
Tamarin Prover	Analyze and support of security protocols	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
Veins	Vehicular network simulation	Tool	Intelligent Transportation Systems	Internet of Vehicles (IoV)
Android Emulator	Android Emulator	Tool	RAN & Mobile Devices	5G and 6G Security
asn1c tool	ASN.1 Compiler	Tool	RAN & Mobile Devices	5G and 6G Security
Bettercap	MITM attacks & reconnaissance	Tool	RAN & Mobile Devices	5G and 6G Security
Docker	Containerisation technology	Tool	RAN & Mobile Devices	5G and 6G Security
Hydra	Brute-force password-cracking	Tool	RAN & Mobile Devices	5G and 6G Security
JupyterHub	Pre-configured data science environment	Tool	RAN & Mobile Devices	5G and 6G Security

Kubernetes	Container deployment and management	Tool	RAN & Mobile Devices	5G and 6G Security	Kubernetes, also known as K8s, is an open source system for automating deployment, scaling, and management of containerized applications.	https://kubernetes.io/	Orchestration	Computing Platform	Infrastructure Provisioning and Configuration	Container Orchestration	VETSG uses Kubernetes to orchestrate containerized components, including all 5G core NFs, gNBs, and UEs.		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
Metasploit	Penetration testing	Tool	RAN & Mobile Devices	5G and 6G Security	The world's most used penetration testing framework	https://www.metasploit.com/	Capability	Red Team Operations	Exploitation and Attack Execution	SSH attack	SSH attack Use tools such as metasploit to attack vulnerable SSH services		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
MongoDB	NoSQL document database	Tool	RAN & Mobile Devices	5G and 6G Security	MongoDB is a document (NoSQL) database designed for ease of Development & Debugging and scaling.	https://www.mongodb.com/	Capability	Data Storage	NoSQL Database	Datastorage for userdata	Directly use MongoDB without Unified Data Repository (UDR)		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
OAI's gNB emulator	5G software stack	Technology Stack	RAN & Mobile Devices	5G and 6G Security	Currently, the OAI platform includes a full software implementation of the 3GPP 4G-LTE and 5G-NR protocol stack for: the RAN (OpenAirInterface5G) for 4G and 5G, the EPC (OpenAirCN) for 4G, the 5G-CORE (or CN-5G) for 5G.	https://openairinterface.org/oai-5g-ran-project/	Capability	Scenario	Infrastructure	3GPP-Stack Implementation	A 5G RAN consists of one or more gNBs. The current implementation of VETSG uses OAI's gNB emulator due to its full support for 5G-NR protocol stack as well as our familiarity with its code base from our previous projects		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
OAuth 2.0	protocol for authorization	Protocol	RAN & Mobile Devices	5G and 6G Security	OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.	https://oauth.net/2/	Capability	Portal Services	Identity & Access Management (IAM)	Service Provider Access	Currently VETSG has implemented the former approach where the NRF acts as an authorization server to grant OAuth 2.0 access tokens [29] to consumer NFs for using services from provider ones.		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
Openapi-generator	Generation of API client libraries	Tool	RAN & Mobile Devices	5G and 6G Security	OpenAPI Generator allows generation of API client libraries (SDK generation), server stubs, documentation and configuration automatically given an OpenAPI Spec (both 2.0 and 3.0 are supported).	https://github.com/OpenAPITools/openapi-generator	Capability	Scenario	Infrastructure	Generate both client and server code of each Network Function	The OpenAPI 3.0 specifications of these APIs for Release 16 have been archived here [11] in YAML format. From these YAML files, we use openapi-generator [12] with option rust-server to generate both client and server code of each NF in Rust.		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
P4 BMv2 software switch	Open-source virtual switch	Tool	RAN & Mobile Devices	5G and 6G Security	bmv2 is not meant to be a production-grade software switch. It is meant to be used as a tool for developing, testing and debugging P4 data planes and control plane software written for them.	https://github.com/p4lang/behavioral-model	Capability	Scenario	Infrastructure	Switch emulation	Responsible for interconnections between RANs and Data Networks (DNs), packet routing/forwarding/inspection, QoS management, and usage reporting.		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
sFuzz	Black-box fuzzing	Tool	RAN & Mobile Devices	5G and 6G Security	In the same vein as the Generic Protocol Framework, sfuzz is a really simple to use black box testing suite called Simple Fuzzer (what else would you expect?). The goal is to provide a simple to use, but fairly powerful and flexible black box testing utility.	https://www.kali.org/tools/sfuzz/	Capability	Red Team Operations	Vulnerability Management	Test 5G NFs with Fuzzing	Use tools such as wfuzz and sfuzz to fuzz test 5G core NFs		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
Tcpdump	Command-line packet analyzer	Tool	RAN & Mobile Devices	5G and 6G Security	A powerful command-line packet analyzer; and libpcap, a portable C/C++ library for network traffic capture.	https://www.tcpdump.org/	Capability	Monitoring and Analytics	Data Collection	Network Traffic Capture	Result collection. We include a statically linked tcpdump binary in all 5G core NF containers to collect network traffic.		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
wfuzz	Web Application fuzzing	Tool	RAN & Mobile Devices	5G and 6G Security	Wfuzz has been created to facilitate the task in web applications assessments and it is based on a simple concept: it replaces any reference to the FUZZ keyword by the value of a given payload.	https://github.com/xmendez/wfuzz	Capability	Red Team Operations	Vulnerability Management	Test 5G NFs with Fuzzing	Use tools such as wfuzz and sfuzz to fuzz test 5G core NFs		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
Wireshark	Network Traffic Analysis	Tool	RAN & Mobile Devices	5G and 6G Security	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Red Team Operations	Network Scanning and Reconnaissance	Packet Capture and Analysis	Packet capture and analysis		Attack Impact Assessment	Cyber Security Excersises	Testbed Design, Testbed Evaluation	TB	This work presents VETSG, a new virtual end-to-end testbed for 5G network security research experiments or training activities such as Capture-The-Flag competitions. In our experiments we demonstrate how to use VETSG for two attack scenarios in 5G networks as well as its performance when it is used in a 5G hacking project for a Mobile Systems Security course.	VETSG: A Virtual End-to-End Testbed for 5G Network Security Experimentation	2022-08	https://dl.acm.org/doi/10.1145/3546096.3546111	7
Controller Area Network (CAN)	High-integrity serial bus system	Protocol	Intelligent Transportation Systems	In-vehicle networks	A controller area network (CAN) bus is a high-integrity serial bus system for networking intelligent devices. CAN busses and devices are common components in automotive and industrial systems.	https://www.bosch-semiconductors.com/products/ip-modules/can-protocols/	Capability	Scenario	Infrastructure	CAN network simulation	VitroBench fully exposes realistic message frames across multiple CAN networks without requiring an actual car.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
LIN	Automotive communication	Protocol	Intelligent Transportation Systems	In-vehicle networks	The Local Interconnect Network (LIN) bus and Controller Area Network (CAN) bus are communications protocols commonly used in automotive and industrial systems. While LIN and CAN serve similar purposes, there are notable differences in their architectures and capabilities.	https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/introduction-to-the-local-interconnect-network-lin-bus.html?srsltid=AfmBOorDSBEIES3OgBOUFLC6wU_A8IHlwdMribNc_lVtlG3LEyj-thR-	Capability	Scenario	Infrastructure	In-vehicle-networks Communication	The communication board is used to communicate between the testbed and the software component. It supports multiple IVN protocols e.g., CAN, CAN-FD and LIN.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
SavvyCan	CAN bus reverse engineering	Tool	Intelligent Transportation Systems	In-vehicle networks	SavvyCAN is a cross platform QT based C++ program. It is a CAN bus reverse engineering and capture tool. It was originally written to utilize EVTV hardware such as the EVTVDue and CANDue hardware. It has since expanded to be able to use any socketCAN compatible device as well as the Macchina M2 and Teensy 3.x boards.	https://savvycan.com/	Capability	Monitoring and Analytics	Analysis & Verification	GUI-based CAN analysis	We perform frame injection via a virtual SocketCAN interface, which is available in Linux. This interface is then accessed like any TCP/UDP socket from Python or other software such as Wireshark, SavvyCan, etc.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
scapy	Python packet manipulation	Library	Intelligent Transportation Systems	In-vehicle networks	Scapy is a powerful interactive packet manipulation library written in Python.	https://scapy.net/	Capability	Red Team Operations	Vulnerability Management	CAN message bridging and fuzzing	Testing Scenarios: The workstation executes the programs for the different test scenario - Python programs are written for bridging and fuzzing. The programs are using scapy CANSocket for receiving and transmitting CAN messages.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
TSMaster	Simulation analysis of automotive buses and ECUs	Tool	Intelligent Transportation Systems	In-vehicle networks	Simulation Analysis of Automotive Buses and ECUs	https://tosunai.us/tsmaster/	Capability	Monitoring and Analytics	Analysis & Verification	Automotive bus monitoring and logging	For sniffing and logging of messages, we leverage TSMaster – an open environment for automotive bus monitoring, testing and logging. The TSMaster display can be customized with graphical meters for speed and RPM, real time parameter values, message traces, decoding using DBC file, and saving to log files of BLF format.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
VXDIAG VCX Professional Car Diagnostic	Vehicle diagnostics	Tool	Intelligent Transportation Systems	In-vehicle networks	A diagnostic tool supporting multiple car brands for vehicle diagnostics and programming.	https://vxdiag.com/	Core Technology	Monitoring and Analytics	Analysis & Verification	Automotive diagnostic	We select VXDIAG VCX Professional Car Diagnostic4 as the diagnostic tool. This is because the diagnostic tool supports several car models, including BMW.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
Wireshark	Network Traffic Analysis	Tool	Intelligent Transportation Systems	In-vehicle networks	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Monitoring and Analytics	Analysis & Verification	CAN frame analysis	We perform frame injection via a virtual SocketCAN interface, which is available in Linux. This interface is then accessed like any TCP/UDP socket from Python or other software such as Wireshark, SavvyCan, etc.		Threat and Vulnerability Assessment, IDS/IPS-Algorithm Development, Attack Impact Assessment		Testbed Design	TB	In this paper, we present VitroBench, a comprehensive test platform involving commercial off-the-shelf (COTS) ECUs that allows arbitrary packet control over IVN. In contrast to existing automotive testbed, an appealing feature of VitroBench is that it allows replication of driving use cases and scenarios directly on the testbed involving COTS ECUs.	VitroBench: Manipulating in-vehicle networks and COTS ECUs on your bench: A comprehensive test platform for automotive Cyber Security research	2023-07	https://www.sciencedirect.com/science/article/pii/S2214209623000797	3
Docker	Containerisation technology	Tool	RAN & Mobile Devices	5G and 6G Security	Docker Engine is an open source Containerisation technology for building and containerizing your applications.	https://www.docker.com/	Core Technology	Computing Platform	Containerisation		For orchestration, the testbed employed a Kubernetes cluster (v1.25) with Docker containers managed via Helm charts.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Helm	Chart repositories	Tool	RAN & Mobile Devices	5G and 6G Security	At a high level, a chart repository is a location where packaged charts can be stored and shared. The distributed community Helm chart repository is located at Artifact Hub and welcomes participation. But Helm also makes it possible to create and run your own chart repository. This guide explains how to do so. If you are considering creating a chart repository, you may want to consider using an OCI registry instead.	https://github.com/Orange-OpenSource/towards5gs-helm	Orchestration	Computing Platform	Container Orchestration	Infrastructure Provisioning and Configuration	For orchestration, the testbed employed a Kubernetes cluster (v1.25) with Docker containers managed via Helm charts.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Kubernetes	Container deployment and management	Tool	RAN & Mobile Devices	5G and 6G Security	Kubernetes, also known as K8s, is an open source system for automating deployment, scaling, and management of containerized applications.	https://kubernetes.io/	Orchestration	Scenario	Infrastructure	Containerized microservices	These components are deployed as containerized microservices within a Kubernetes-managed environment to achieve portability, fault isolation, and dynamic scalability.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
MITRE CAPEC	Attack Pattern Enumerations and Classifications	Tool	RAN & Mobile Devices	5G and 6G Security	Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.	https://capec.mitre.org/	Capability	Blue Team Operations	Vulnerability Management	Fine-tuning model data, Inference result validation	This model receives CVE descriptions and maps them to corresponding Common Weakness Enumeration (CWE) categories and CAPEC identifiers		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
MITRE CWE	Weaknesses repository	Tool	RAN & Mobile Devices	5G and 6G Security	Knowing the weaknesses that result in vulnerabilities means software developers, hardware designers, and security architects can eliminate them before deployment, when it is much easier and cheaper to do so	https://cwe.mitre.org/	Capability	Blue Team Operations	Vulnerability Management	Fine-tuning model data, Inference result validation	Each inference result from the VWA inference rApp is cross-validated against the MITRE CWE JSON reference repository.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
NumPy	Scientific computing	Library	RAN & Mobile Devices	5G and 6G Security	NumPy is the fundamental package for scientific computing in Python. It is a Python library that provides a multidimensional array object, various derived objects (such as masked arrays and matrices), and an assortment of routines for fast operations on arrays, including mathematical, logical, shape manipulation, sorting, selecting, I/O, discrete Fourier transforms, basic linear algebra, basic statistical operations, random simulation and much more	https://numpy.org/	Capability	Custom Development	AI & Machine Learning	Data preprocessing and handling	Supporting libraries such as NumPy and Pandas facilitated data preprocessing and handling.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
NVD	Vulnerability repository	Tool	RAN & Mobile Devices	5G and 6G Security	The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics.	https://nvd.nist.gov/	Capability	Blue Team Operations	Vulnerability Management	Common Vulnerabilities and Exposures (CVE) information for trivy	This model receives CVE descriptions and maps them to corresponding Common Weakness Enumeration (CWE) categories and CAPEC identifiers		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
O-RAN SC	Creation of software for the Radio Access Network (RAN).	Tool	RAN & Mobile Devices	5G and 6G Security	The O-RAN Software Community (SC) is a collaboration between the O-RAN ALLIANCE and Linux Foundation with the mission to support the creation of software for the Radio Access Network (RAN). The RAN is the next challenge for the open source community. The O-RAN SC plans to leverage other LF network projects, while addressing the challenges in performance, scale, and 3GPP alignment.	https://o-ran-sc.org/	Capability	Scenario	Infrastructure	RAN implementation	Adding to these challenges, prevailing security frameworks developed for 5G networks fall short in addressing the specific requirements of the open and distributed 6G O-RAN landscape.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Pandas	Data analysis and manipulation	Library	RAN & Mobile Devices	5G and 6G Security	Pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language.	https://pandas.pydata.org/	Capability	Custom Development	AI & Machine Learning	Data preprocessing and handling	Supporting libraries such as NumPy and Pandas facilitated data preprocessing and handling.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
PyTorch	Deep learning library	Library	RAN & Mobile Devices	5G and 6G Security	PyTorch is an optimized tensor library for deep learning using GPUs and CPUs.	https://pytorch.org/	Capability	Custom Development	AI & Machine Learning	AI model development	The AI model was developed using Python 3.10 with the PyTorch deep learning framework (v2.2.1+cu121) for training and inference, along with the Hugging Face Transformers library (v4.40) providing a pre-trained BERT language model.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Transformers	Pretrained AI models	Library	RAN & Mobile Devices	5G and 6G Security	Transformers provides APIs and tools to easily download and train state-of-the-art pretrained models. Using pretrained models can reduce your compute costs, carbon footprint, and save you the time and resources required to train a model from scratch. These models support common tasks in different modalities, such as:	https://huggingface.co/docs/transformers/	Capability	Custom Development	AI & Machine Learning	AI model development	The VWA inference rApp serves as the system's analytical core. It incorporates a fine-tuned semantic inference model based on the Bidirectional Encoder Representations from Transformers (BERT) architecture. This model receives CVE descriptions and maps them to corresponding Common Weakness Enumeration (CWE) categories and CAPEC identifiers.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Trivy	Vulnerabilities (CVE) & misconfigurations (IaC) Scanner	Tool	RAN & Mobile Devices	5G and 6G Security	Use Trivy to find vulnerabilities (CVE) & misconfigurations (IaC) across code repositories, binary artifacts, container images, Kubernetes clusters, and more. All in one tool!	https://trivy.dev/latest/	Capability	Blue Team Operations	Vulnerability Management	CVE Scanner	The CVE Scanner rApp performs systematic vulnerability assessments of deployed xApps using the Trivy engine. Trivy interfaces with the National Vulnerability Database (NVD) (NVD, 2024) to retrieve current Common Vulnerabilities and Exposures (CVE) information.		Cyber Security Evaluation: Security-Monitoring and Vulnerability management			TB	To address these issues, this study proposes the Vulnerability Weakness Attack for 6G (VWA-6G) system, an artificial intelligence (AI) assisted framework for continuous security monitoring. This framework utilizes a contextually fine-tuned BERT-based model. The VWA-6G AI model automates semantic mapping from Common Vulnerabilities and Exposures (CVEs) to Common Weakness Enumerations (CWEs) and Common Attack Pattern Enumerations and Classifications (CAPECs), leveraging specialized datasets derived from forward-looking 6G technical materials.	VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration	2025-06	https://www.sciencedirect.com/science/article/pii/S016740482500255X	0
Google Cloud	Cloud computing services	Platform	ICS	Water Systems	Google Cloud is a suite of cloud computing services offered by Google, providing infrastructure, platform, and software as a service (IaaS, PaaS, SaaS) solutions.	https://cloud.google.com/	Core Technology	Computing Platform	Cloud Infrastructure		Infrastructure Provisioning and Configuration	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of cybersecurity professionals with knowledge of water-focused ICS cybersecurity.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
Modbus	Communication protocol for industrial devices	Protocol	ICS	Water Systems	It is used to establish client-server communication between intelligent devices. It is a de facto standard, truly open and the most widely used network protocol in the industrial manufacturing environment.	https://modbus.org/	Capability	Scenario	Infrastructure	Industrial Communication	Industrial Communication	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
modpoll	Modbus master simulator	Tool	ICS	Water Systems	Command line based Modbus master simulator and test utility	https://www.modbusdriver.com/modpoll.html	Capability	Scenario	Traffic Generation	Simulates MODBUS traffic	Simulate MODBUS traffic	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
OpenPLC	Open-source programmable logic controller	Tool	ICS	Water Systems	OpenPLC is an open-source Programmable Logic Controller that is based on an easy to use software. It is the first fully functional standardized open source PLC, both in software and in hardware.	https://www.openplcproject.com/	Capability	Scenario	Infrastructure	PLC Device Simulation	Simulate PLC devices	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
PfSense	Firewall and routing platform	Tool	ICS	Water Systems	Open-source firewall and router platform based on FreeBSD.	https://www.pfsense.org/	Capability	Blue Team Operations	Firewalls & Network Security Gateways	Firewall and Routing Configuration Scenario	Opportunity to practice configuring firewalls for the Enterprise and ICS network perimeters	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
PyModbus	Modbus protocol implementation in Python	Library	ICS	Water Systems	Pymodbus is a full Modbus protocol implementation offering client/server with synchronous/asynchronous API and simulators.	https://github.com/pymodbus-dev/pymodbus	Capability	Scenario	Infrastructure	Communication with PLCs	Simulation of the HIL implementation for the physical components, including I/O	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
ScadaBR	Open-source SCADA system	Tool	ICS	Water Systems	Open-source SCADA (Supervisory Control and Data Acquisition) system for industrial automation	http://www.scadabr.com.br/	Capability	Scenario	Infrastructure	SCADA System Implementation	The Supervisory Control and Data Acquisition (SCADA) machine was implemented using the Open Source software ScadaBR	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
VMWare vSphere	Virtualization platform	Tool	ICS	Water Systems	The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.	https://www.vmware.com/products/cloud-infrastructure/vsphere	Core Technology	Computing Platform	Virtualization platform/Type-1-Hypervisor		Infrastructure Provisioning and Configuration	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of cybersecurity professionals with knowledge of water-focused ICS cybersecurity.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
Windows Active Directory	Centralized authentication and authorization system	Platform	ICS	Water Systems	Microsoft service for managing users, computers, and permissions within a network. It provides authentication, centralized policy enforcement, and role-based access control for enterprises.	https://learn.microsoft.com/de-de/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview	Capability	Portal Services	Identity & Access Management (IAM)	Enterprise Domain Controller	Enterprise domain controller for the vWaterLabs testbed	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1
Wireshark	Network Traffic Analysis	Tool	ICS	Water Systems	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.	https://www.wireshark.org/	Capability	Blue Team Operations	Network Analysis & Reconnaissance	ICS Network Traffic Analysis	Examine ICS network traffic	Instructional Design	Threat and Vulnerability Assessment		Testbed Design, Cost effective Cyber Range Design	TB	Help rapidly increase the training and education of Cyber Security professionals with knowledge of water-focused ICS Cyber Security.	vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education	2021-04	https://dl.acm.org/doi/10.5555/3470135.3470138	1