

Review

A Review of Cyber-Ranges and Test-Beds: Current and Future Trends

Elochukwu Ukwandu ¹, Mohamed Amine Ben Farah ², Hanan Hindy ³, David Brosset ⁴,
Dimitris Kavallieros ^{5,6}, Robert Atkinson ², Christos Tachtatzis ², Miroslav Bures ⁷,
Ivan Andonovic ² and Xavier Bellekens ^{2,*}

¹ Department of Computer Science, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2YB, UK; eaukwandu@cardiffmet.ac.uk

² Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow G1 1XQ, UK; mohamed.ben-farah@strath.ac.uk (M.A.B.F.); robert.atkinson@strath.ac.uk (R.A.); christos.tachtatzis@strath.ac.uk (C.T.); ivan.andonovic@strath.ac.uk (I.A.)

³ Division of Cybersecurity, Abertay University, Dundee DD1 1HG, UK; 1704847@abertay.ac.uk

⁴ Naval Academy Research Institute, Arts et Métiers Institute of Technology, Rue du Poulmic, 29160 Lanvéoc, France; david.brosset@ecole-navale.fr

⁵ The Center for Security Studies (KEMEA), GR-101 77 Athens, Greece; d.kavallieros@kemea-research.gr

⁶ Department of Informatics and Telecommunications, University of Peloponnese, 221 00 Tripoli, Greece

⁷ Department of Computer Science, Faculty of Electrical Engineering, Czech Technical University in Prague, 166 36 Prague 6, Czech Republic; buresm3@fel.cvut.cz

* Correspondence: xavier.bellekens@strath.ac.uk

Received: 13 October 2020; Accepted: 5 December 2020; Published: 13 December 2020



Abstract: Cyber situational awareness has been proven to be of value in forming a comprehensive understanding of threats and vulnerabilities within organisations, as the degree of exposure is governed by the prevailing levels of cyber-hygiene and established processes. A more accurate assessment of the security provision informs on the most vulnerable environments that necessitate more diligent management. The rapid proliferation in the automation of cyber-attacks is reducing the gap between information and operational technologies and the need to review the current levels of robustness against new sophisticated cyber-attacks, trends, technologies and mitigation countermeasures has become pressing. A deeper characterisation is also the basis with which to predict future vulnerabilities in turn guiding the most appropriate deployment technologies. Thus, refreshing established practices and the scope of the training to support the decision making of users and operators. The foundation of the training provision is the use of Cyber-Ranges (CRs) and Test-Beds (TBs), platforms/tools that help inculcate a deeper understanding of the evolution of an attack and the methodology to deploy the most impactful countermeasures to arrest breaches. In this paper, an evaluation of documented CR and TB platforms is evaluated. CRs and TBs are segmented by type, technology, threat scenarios, applications and the scope of attainable training. To enrich the analysis of documented CR and TB research and cap the study, a taxonomy is developed to provide a broader comprehension of the future of CRs and TBs. The taxonomy elaborates on the CRs/TBs dimensions, as well as, highlighting a diminishing differentiation between application areas.

Keywords: Cyber-Ranges; Test-Beds; Cyber-Security; threat simulations; training; education; scenario; virtual environment; cyber-situation awareness; taxonomy

1. Introduction

In the recent past, a proliferation in the number and complexity of cyber-security incidents with deeper consequences has become evident as attackers become more skilled, sophisticated and

persistent. The extent of cyber-incidents targeting critical infrastructures and the public has been fueled by global events such as the Stuxnet worm [1]. This attack targeted numerous centrifuges in Iran's Natanz uranium enrichment facility from where it spread across many countries, impacting numerous organisation's critical infrastructure and fueling a clear and immediate need for increased and new dimension in cyber-situational awareness [2]. The consequences of these types of attack brought in what the cyber-security research community referred to as a 'game changer' in cyber-attack dynamics, highlighting the strong need for personnel training [3–5]. Furthermore, in the recent past, the cyber-security industry has undergone a significant shift in respect of acknowledging the importance of security training of users, transitioning from "users are the weak link of cyber-security" towards "users can be trained like muscles hence, improving a company's overall security posture" [6,7]. The evolving change of stance is a fundamental trigger for change in cyber-security procedures, in turn stimulating a growing demand for training platforms. Cyber-Ranges (CR) are defined by the National Institute of Standards and Technology (NIST) as "interactive and simulated representations pertaining to an organization's local network, system, tools, and applications" [8], whereas Test-Beds (TB) are defined as "a configurable and extensible cyber range with simulated industrial processes" [9]. CR provide real-world platforms for training Information and Communication Technology (ICT) professionals against a wide range of cyber-attacks and cyber-warfare scenarios. TB enable the training of Operational Technology (OT) network personnel facing cyber-attacks to improve cyber-situational awareness. CR and TB are complementary as OT and ICT networks are interlacing with advances in communications, adoption of the Internet of Things (IoT) and Industrial IoT (IIoT) across various sectors [10,11]. Scenarios replicating a spectrum of cyber-attacks can be established, enhancing the training of operators and users within recognisable environments in the identification of, and mitigation strategies to arrest cyber-breaches. Training in an emulated environment accelerates effective learning of best practice and the 'real-time' dynamic interaction promotes a deeper understanding of the consequences of any action [12]. CR/TB facilitate the establishment of an extended range of attack scenarios with varying levels of complexity, governed by the stage of training. Groups of users can also train on a remotely accessible platform to define, optimise and evaluate the impact of a coordinated response to cyber-attacks, e.g., 'blue team', 'red team', back and 'front office' of (say) a bank. Group training involving multiple teams comprising varying knowledge sets enhance the cyber-situational awareness of the organisation and improve the response time to identify and arrest a cyber-attack.

In response to the pressuring demand to respond to exponentially evolving cyber-attacks, this paper presents an extensive and thorough analysis of CRs and TBs based on the recent prominent research and manuscripts. To the best of the authors knowledge, this thorough analysis is not available in the literature, thus limiting the presence of an adequate resource for researchers. Moreover, to complete the study, two taxonomies targeted towards the different dimensions of CRs and TBs are developed and presented in this manuscript.

The remainder of the paper is organised as follows. Section 2 details the methodology applied to execute on a review of the state-of-the-art in CRs/TBs; Section 3 presents a summary of existing knowledge in the disciplines. Section 4 provides a critical assessment on reported CRs/TBs classified by the domain of applications, user classes, method of experimentation and implementation. Section 5 covers the scenarios and applications of CRs/TBs. Section 6 focuses on CR/TB taxonomies informed by the findings of the review. Section 7 describes the training methods implemented through CRs/TBs. Section 8 elaborates on the future evolution and use of CRs/TBs, providing evidence of the narrowing gap between their different application areas. Conclusions are drawn in Section 9.

2. Methodology

This section provides detailed of how the review was conducted and method used.

2.1. Overview

The review presented here adopts a systematic methodology based selection, extraction, and execution in line with the guidance prescribed by Okoli and Schabram in [13] and Okoli in [14]. The review is stand-alone focusing on existing knowledge, evaluation, and synthesis in the domains of CR and TB, the principle aim being to provide evidence of the growing density of cyber-attacks automation using modern technologies with increasing levels of stealth and sophistication in both landscape and execution. Furthermore, the increasing degrees of network inter-connectivity as a consequence, for example, of emerging Industry 4.0 ‘smart-everything’ scenarios and the concomitant changes in the dynamics and scope of the threat surface, translates into a major challenge in determining evolving cyber situational awareness for researchers, educators, and trainers. The prediction of future trends, scenarios, and possible application areas using current operational environments presents significant challenges. Therefore, this paper, a study with these aims has not been reported to date. This paper, hence projects the training requirements for cyber situational awareness within these evolving infrastructures by utilising the existing knowledge within the literature and current sector practices as the seed.

2.2. Aim and Objectives

The literature review aims to identify and analyse the current state-of-the-art in the use and applications of CRs/TBs within cyber-security training and map the range of applications provisioned by these platforms. The objectives are as follows:

- Survey recent CR and TB research.
- Analyse and review state-of-the-art trends, scenarios and applications.
- Establish a taxonomy for future CRs/TBs.
- Equip cyber-security professionals with the relevant skills to combat cyber-threats in next-generation highly inter-connected, multi-domain infrastructures.

2.3. CRs and TBs Survey

A comprehensive literature review of the state-of-the-art in CRs/TBs disciplines was carried out to establish a reference of current platform features and training tools, the foundation for the development of the main contributions presented in the paper.

2.3.1. Classification and Research Criteria

As CR and TB migrate towards convergence, the literature search used the following keywords to surface the most relevant publications:

1. “Cyber-ranges” + (“Military” + “Defense” + “Intelligence”) or (“Industry” + “Commercial”) or (“Education” + “Research”)
2. “Test-bed” + (“IoT” or “Smart Grid” or “Cloud”) + cyber

Furthermore, the review only considered papers published within the last 5 years of 2015–2020.

2.3.2. Selection Criteria

Searches in five databases were executed: ScienceDirect, IEEE Explore, Springer, Wiley, and ACM. However, fundamental research relevant to the study outwith the specified search period were taken into consideration. The graphs presented in Figure 1a–c depict the evolution of the number of publications from 2015 to 2020 on Test-beds in the Internet-of-Things (IoT), Smart Grid and Cloud disciplines. Increases in the number of publications for all domains is clearly evident, demonstrating extensive research in cyber-security and Test-beds [15].

2.3.3. Extraction Criteria And Results

The review was restricted further to consider only the current dominant area of application for TBs—Smart Grids—and the future area of IoT/smart devices, driven by the goal of predicting future requirements seeded by the current state-of-the-art.

Figures 1d–i and 2a–c present the results of the review; Figure 1d–i summarise the publication types in Test-bed within the Springer and ScienceDirect databases. The percentage of papers on IoT Test-beds from the Springer database in Figure 1d shows that 25% of publications are journal articles, while 44% are conference papers; 11% of papers were published in conferences proceedings in Smart Grids (Figure 1e); those published in the Cloud domain represent the highest percentage at (80%) (Figure 1f).

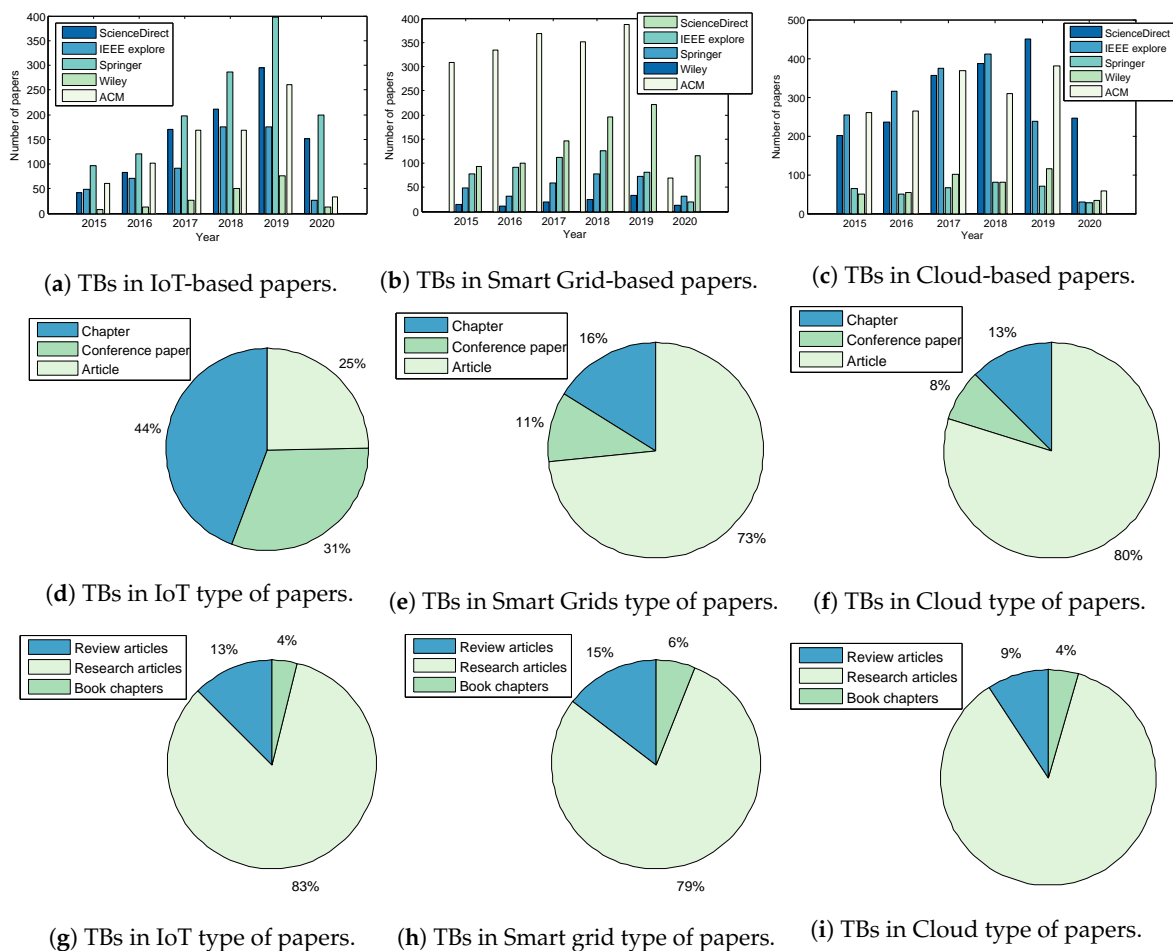


Figure 1. Types of publications in TBs between 2015 and 2020 in Springer and ScienceDirect database respectively.

Similarly, the review for CRs was restricted to the current prominent applications areas within Military, Defence and Intelligence (Military), Education and Research (Education), and Industry and Commercial sectors (Industry). The data targeted focused on gaining insights on threat dynamics/proliferation, and emerging countermeasure strategies, a foundation for predicting future trends, technologies, and application areas.

On inspection of Figure 2, it is evident that ACM publishes a greater number of papers in relation to CRs with progressive growth in number from 2015 through to 2019 (Figure 2a). Journal articles account for 64% of publications, book chapters 25% and conference proceedings 11% (Figure 2b). Also clear is that researched-based articles are more readily accepted for publication at a rate of 82% compared to other types of articles such as Book Chapters at 13% and Review articles at 5% (Figure 2c).

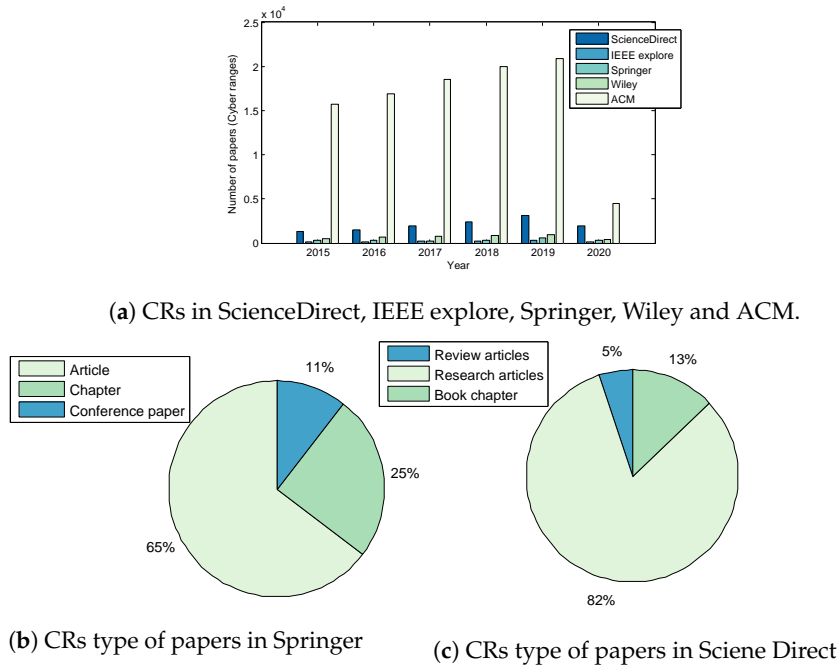


Figure 2. Evolution and classification of CRs publications.

Further, ACM has published more Cyber-range related papers in the three domains of Military, Education, and Industry, followed by Wiley, ScienceDirect, Springer and IEEE (Figure 3). Cyber-range papers published in ACM are predominately in Education, followed by Industry and then Military. Wiley, ScienceDirect, Springer, and IEEE published more Industry-related Cyber-range papers than those in Education and Military.

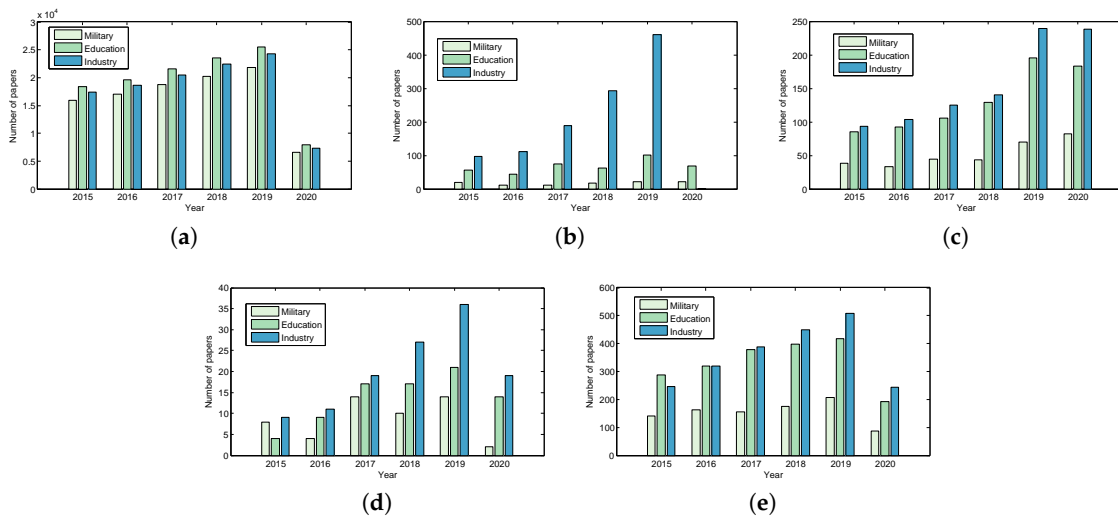


Figure 3. (a) CR in ACM (b) CR in ScienceDirect (c) CR in Springer (d) CR in IEEE (e) CR in Wiley.

3. Related Work

CR and TB solutions have been applied in both commercial and public settings such as the military/defence, intelligence, education, research, and training [16]. The extensive usage is driven by the need to be cyber-security prepared against persistent threats to critical infrastructures and businesses. The first publicly reported CR was the National Cyber-Range (NCR) [17], created by the US Department of Defence. However, as described in [17], other ‘stealthy’ CRs and TBs existed across the world for cyber-warfare training in advance of the NCR.

Leblanc et al. [18] surveyed the state-of-the-art of 13 simulation-centric CRs categorising them into private, academic or public sector research. The review, while useful, dates back to 2011 and given the significant advances in the functionality of technologies and complexity of threat dynamics limits the value of their findings in the goal of predicting the future evolution.

Davis and Magrath in [16] conducted a survey of CRs in the public domain focusing on 30 existing systems in 2013. The review focused primarily on the merits of each approach in respect of their functionalities with emphasis on cost-effectiveness. The classification was segmented in terms of military and government; academic; and commercial and further categorised as either simulation or emulation-driven implementations. The authors concluded that emulation-driven CRs utilised TBs and were proven to be effective environments for training and test. The trade-off between highly functional, robust training environments and the concomitant cost implications as a result of the complexity of the implementations was stressed. Inherent within the trade-off, is the provision for the sharing of resources and/or virtualisation. Conversely, simulation-based CRs are implemented solely through software that model real world scenarios, and are thus easily scalable. However, emulation-driven CRs can be validated more readily for performance [16].

As the review [16] was carried out considering CRs and TBs before 2013, the conclusions on the trade-off between functionalities and cost-effectiveness has limited value in the determination of the future evolution of the platforms.

Priyadarshini [19] also reported the results of a review on CRs in 2018, culminating in the definition of the features and capabilities of an 'Ideal CR'; the components, scenarios, and capabilities of the CR at the University of Delaware (CRUD) were used as the foundation for the definition of the future platform. The bench-marking did not consider the needs of the applications viz. to facilitate training, education, and research addressing recent and future threat profiles, their proliferation and modes of attack.

The most recent literature by Yamin et al. [20] reviews unclassified CRs and security TBs. The authors propose a taxonomy with reference to the architecture, scenarios, capabilities, roles, and tools as the criteria. The main output is a proposed baseline to aid the development and evaluation of CRs.

The above reviews provided valuable insights into CR/TB technologies with potential to facilitate training in the management of persistent cyber-threats, their changes in perspective, execution, and patterns. However, as a consequence of the dynamic and rapid development of technologies and the enhanced capabilities they provide, the conclusions are limited in the goal of predicting the evolution of future CR/TB platform capabilities and the scope of training they support. The taxonomy that captures these dynamic trends needs to be re-established in the light of advances made in the recent past.

4. Systematic Review

A systematic review to bring to fore the context of this paper is presented using this section.

4.1. Cyber-Ranges and Test-Beds

Table 1 is a summary of CRs and TBs covering a period of five years, the basis for a systematic review to predict the threat landscape, dimension and proliferation taking into consideration continual technological advancement. The Table is segmented into a number of categories viz. Military, Defense and Intelligence (MDI), Academic (Aca), Enterprise and Commercial (EC), Service Providers (SP), Open Source (OS), Law Enforcement (LE), Government (Gvt), Mode of Deployment (Deploy), Area of Specialties (Specialty), Types (Type), The Team it supports (Team), The Testing Environment (TE) and Method of Experimentation (ME).

Table 1. Summary Table of Related Works.

Categories	Ref	MDI	Aca	EC	SP	OS	LE	Govt	Deploy	Specialty	Type	Team	TE	ME
NCR	[17] [16] [19]	Y	N	N	N	N	N	Y	C, VPN	ST, NS	Fed	R, B, Gy	VM	E
Virginia CR	[21] [19]	N	Y	N	N	N	N	N	C	ST	Pub, Prv	R, B	VM	N
Michigan CR	[19]	N	Y	N	N	N	Y	N	C, VPN	ST, AS, CSE	Pub, Prv	R, B	VM, SB	N
Pinecone CR	[19]	N	N	Y	N	N	N	N	N	N	N	N	N	N
IBM X-Force	[19]	N	N	Y	N	N	N	N	C	N	Prv	R, B	VM, SB	N
Cyberbit CR	[19]	N	N	N	Y	N	N	N	N	N	N	N	N	N
Arizona CWR	[19]	N	N	N	N	Y	N	N	N	CSE	N	N	N	N
CRATE	[22] [19]	Y	N	N	N	N	N	N	C, VPN	N	Fed	R, B	VM	N
Cisco CR	[19]	N	Y	Y	N	N	N	N	C, VPN	N	Pub, Prv	R, B, Gn	VM	N
NATO CR	[23] [19]	N	Y	N	N	N	N	N	C, VPN	N	Fed	R, B, G, W, Y	VM, SB	N
DoD CR	[24] [19]	Y	N	N	N	N	N	N	C, VPN	N	Fed	R, B	VM, SB	N
Raytheon CR	[19]	N	N	Y	N	N	N	N	C, VPN	N	Fed	R, B	N	N
Baltimore CR	[19]	N	N	Y	N	N	N	Y	C, VPN	N	Pub, Prv	R, B	N	N
Florida CR	[19]	Y	Y	N	N	N	N	Y	C	PT, EH, NS, SS	Fed, Pub, Prv	R, B	N	N
CRUD	[19]	N	Y	N	N	N	N	N	N	N	N	R, B, P	VM	N
Regent CR	[19]	Y	Y	Y	N	N	N	N	N	RA, M, TV, DF	N	N	N	N
Wayne CR	[19]	N	Y	Y	N	N	N	N	C	EH, CTF, PT, EH	N	N	SB	N
Arkansas CR	[19]	N	Y	N	N	N	N	N	C	PT	N	N	VM	N
Georgia CR	[19]	N	N	Y	N	N	N	Y	N	N	N	N	N	N
SIMTEX	[16]	Y	N	N	N	N	N	Y	N	CSE	Pub	N	N	S
CAAJED	[25] [16]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
SAST	[26] [16]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
StealthNet	[27] [16]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
SECUSIM	[28] [16]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
RINSE	[29] [16]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
NetENGINE	[30] [16]	N	Y	N	N	N	N	Y	N	CSE	Prv	N	N	S
ARENA	[31] [16]	N	Y	N	N	N	N	N	N	CSE	Pub	N	N	S
OPNET-based	[32] [16]	N	N	N	N	N	N	N	N	NA	Pub	N	N	N

Table 1. Cont.

Categories	Ref	MDI	Aca	EC	SP	OS	LE	Govt	Deploy	Specialty	Type	Team	TE	ME
LARIAT	[33] [16]	Y	N	N	N	N	N	N	N	CSE	Pub	N	N	S
VCSTC	[34] [16]	N	Y	N	N	N	N	Y	N	CSE	Pub	N	N	S
Breaking Point	[16]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	S
Exata	[16]	Y	N	Y	N	N	N	N	N	Training	Prv	N	N	S
PlanetLab	[16]	N	N	N	N	N	N	N	N	Training, CSE	Fed, Pub	N	N	O
X-Bone	[16]	N	N	N	N	N	N	N	N	CSE	Prv	N	N	O
JIOR	[16]	Y	N	N	N	N	N	Y	N	CSE, Training	Fed	N	N	E
INL	[35] [16]	Y	N	N	N	N	N	Y	N	CSE, Training	Fed	N	N	E
Emulab	[36] [16]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
DETER	[16]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
Virtualised CR	[37] [16]	N	Y	N	N	N	N	N	N	CSE, Research	Fed	N	N	E
Reassure	[38] [16]	N	Y	N	N	N	N	N	N	Research	Pub	N	N	E
Northrop G	[16]	Y	N	Y	N	N	N	N	N	CSE, Training	Prv	N	N	E
Counter HC	[16]	N	N	Y	N	N	N	N	N	Training, CSE	Prv	N	N	NA
Detica	[16]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	N
ATC	[39] [16]	N	N	Y	N	N	N	N	N	Training	Prv	N	N	LS
Testbed@ TWISC	[40] [20]	N	Y	N	N	N	N	N	C	Research, ST	Prv	N	SB	E
INSALATA	[41] [20]	N	N	N	N	Y	N	N	C	NS, Research	Prv	N	Hybrid	E
CyberVan	[42] [20]	Y	N	N	N	N	N	N	C	ST, NT	Pub	N	Hybrid	S
SoftGrid	[43] [20]	Y	N	N	N	Y	N	N	C	ST, NT, AS	Prv	N	H	E

Legend:

Aca: Academic or Research

AS: Attack Simulation

B: Blue

C: Cloud

CSE: Cyber Security Exercise

CTF: Catch-The-Flag

DF: Digital Forensic

E: Emulation

EC: Enterprise and Commercial

EH: Ethical hacking

Fed: Federated

Gn: Green

Govt: Government

Gy: Grey

H: Hardware

LE: Law Enforcement

M: Monitoring

MDI: Military, Defense and Intelligence

ME: Method of Experimentation

N: No/Not Available

NS: Network Security

O: Overlay

OS: Open Source

P: Purple

Prv: Private

PT: Penetration Testing

Pub: Public

R: Red

RA: Ransomware Attacks

S: Simulation

SB: Sandbox

SP: Service Provider

SS: System Security

ST: Security/Software Testing

TE: Testing Environment

TV: Threat and Vulnerability

VCN: Virtual Clone Network

VM: Virtual Machine

VPN: Virtual Private Network

W: White

Y: Yellow

Y: Yes/Available

- Application Domains:** A total of 44 CRs were categorised, including the CRs surveyed by [16,19]. Figure 4 shows that CRs have been predominantly used for academic purposes in education and research at 31%. The result differs from that of Davis and Magrath [16] of 2013, where the predominant use of CRs was in the training for cyber-security, a paradigm shift in the main application. The trend is also consistent with the findings presented in Section 2; that the bulk of CR papers were published by the academic community reporting on applications in teaching, learning, and research; followed by Enterprises and Commercial organisations, as well as, Military Defence and Intelligence for training purposes such as cyber-defence preparedness both at 24% respectively. The use in of CRs in Government was at 15% rate, while other application areas such as Law Enforcement, Service Providers, and Open-Source constitute only 2% of the manuscripts surveyed.

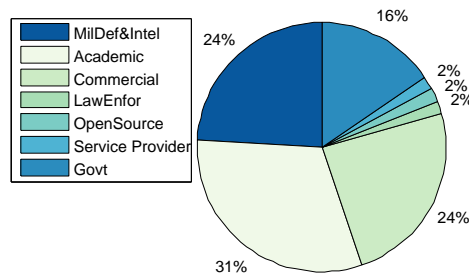


Figure 4. Cyber-Range Domain of Applications.

Only five TBs were identified (Table 1), of which three were applied in academia for the purposes of education and research; Testbed@TWISC [40], CyberVan [42], and INSALATA [41]. SoftGrid [43] and systems such as LARIAT [33,44], have been applied in defence and intelligence training.

- Types:** Figure 5 shows that public and federated CRs are predominant in use at 30% respectively, private at 24%, a combination of Public-Private at 11%, a combination of Federated-Public-Private at 3% and Federated-Public at 2%. A link between the cyber-security preparedness application with the type of technology is evident. The predominant domain of application is for academic purposes and the institutions that provide education and research are mostly public with international collaborative perspectives, thereby suggesting an inter-relationship.

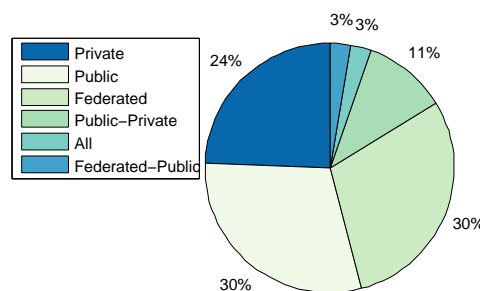


Figure 5. Cyber-Range Types.

CyberVan [42] is a public type of Test-bed, while Testbed@TWISC [40], INSALATA [41], SoftGrid [43] and LARIAT [33,44] are private TBs.

- Team Formation:** Team formations are central to training through exercises emulating operations. Teams are formed depending on the type of exercise; (1) Red team acts as adversaries by launching attacks on the network system; (2) Blue team is responsible for defending against an adversary

attack; (3) White team for administrative management; (4) Purple team sets objectives for offensive and defensive strategies; (5) Green team is responsible for maintaining network efficiency; (6) Grey team conducts non-malicious activity; and (7) Yellow team acts as a motivator during each exercise. From the survey Red-Blue team formation is most prominent at 67%, an indication that many CRs are dedicated to cyber-attack and defence training and exercises, followed by Red-Blue-Grey teams at 9% and others such as Red-Blue-Green, Red-Blue-Green-White-Yellow and Red-Blue-Purple with 8% each as shown in Figure 6. The training of teams on operational environments is restrictive in the scope of threat conditions that can be established as it compromises business continuity.

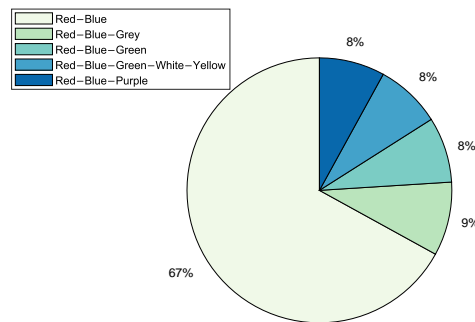


Figure 6. Cyber-Range Teams.

- **Methods of Experimentation:** Figure 7 highlights that simulation is the most common implementation methodology at 60%, followed by emulation at 38%, overlay at 8%, and finally live scenario demonstrations at 4%.

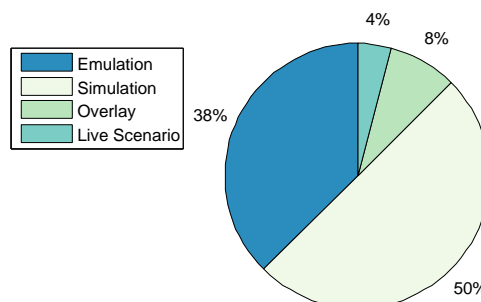


Figure 7. Cyber-Range Methods of Experimentation.

Testbed@TWISC [40], INSALATA [41], SoftGrid [43] and LARIAT [33,44] all use emulation techniques except CyberVan [42] that is based on simulation.

4.2. Technologies

Figures 8 and 9 summarise CR Core technologies segmented as virtualisation, simulation, containerisation, and physical hardware; some CRs provide a combination of these technologies such as virtualisation with physical hardware. TB implementations target the training of cyber situational awareness for domain experts in the areas of control and information technology networks. The platforms also enable training in operational technologies with few employing simulation and emulation but the bulk are based on physical hardware. Table 2 presents an overview of CRs/TBs technologies used based on the available literature with focus on the selected application areas.

4.2.1. Core Technologies

The modelling of certain infrastructures underpinning a particular application require the use of a combination of methods, in effect a hybrid implementation as shown in Figure 10, where the

combination of Virtualisation with Physical Hardware technologies is presented. These combinations enhance the capabilities of CR—by allowing operational and information technologies to be part of a scenario—embody features of both CR and TB.

Containerisation such as Docker is summarised in Figure 11. Containerisation is a light-weight approach to virtualisation, a uniform structure in which any application can be containerised (stored), transported, and deployed (run). Hardware virtualisation, on the other hand, implies Virtual Machine (VM) deployment i.e., a layer between the hardware and the host operating system, managed by a hypervisor as shown in Figure 12. The use of containers is more scalable compared to VMs, but the latter provide a more flexible and secure system. Their application depends largely on need but there is the possibility of VMs and Container technologies merging into a form of cloud portability.

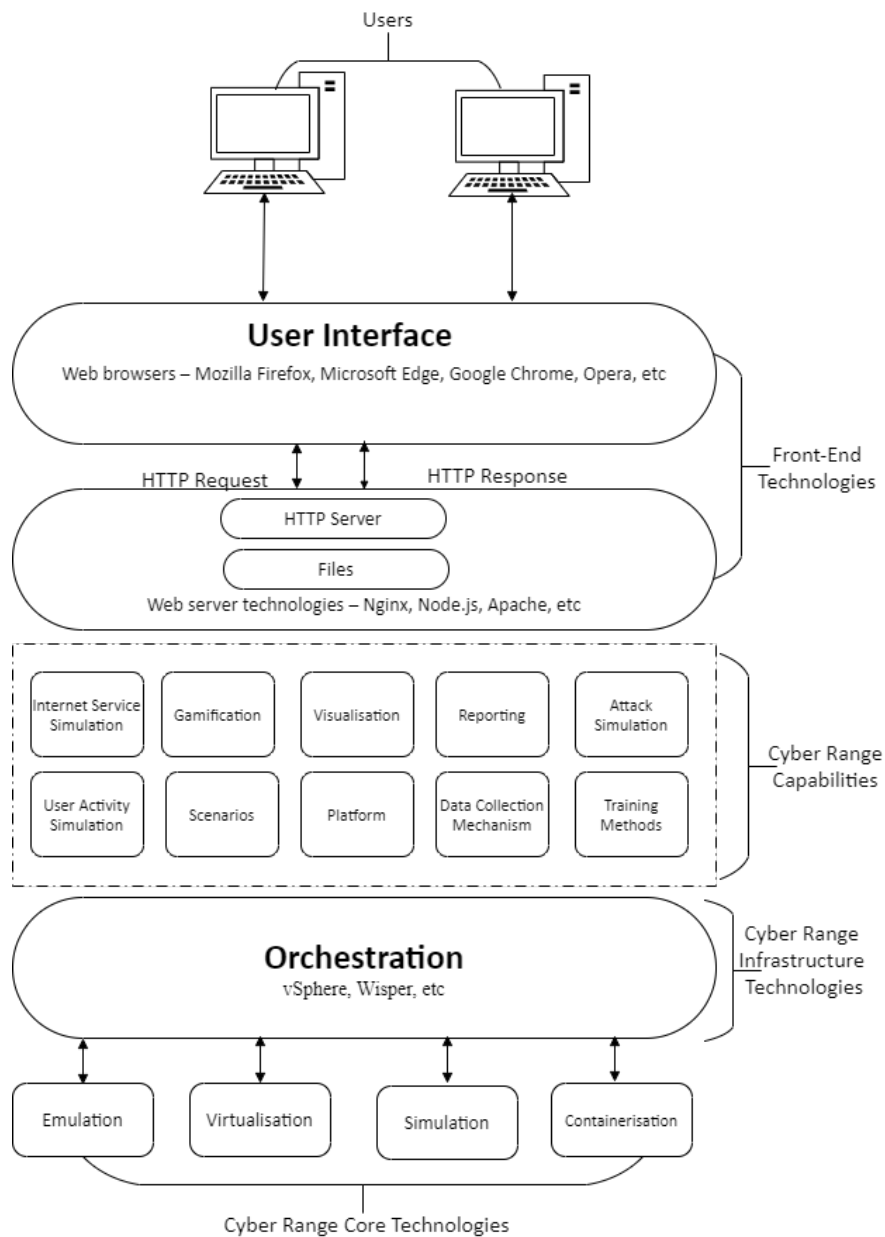


Figure 8. Architectural Design of a Cyber Range.

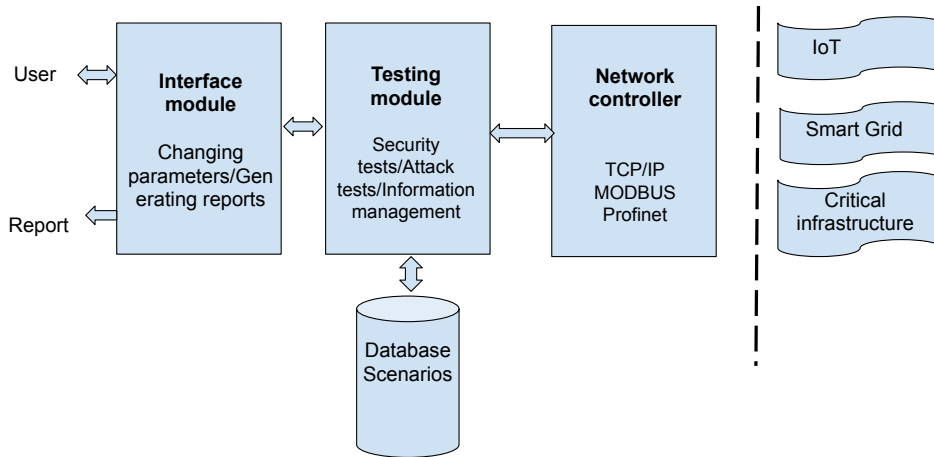


Figure 9. Architectural Design of a Test-Bed.

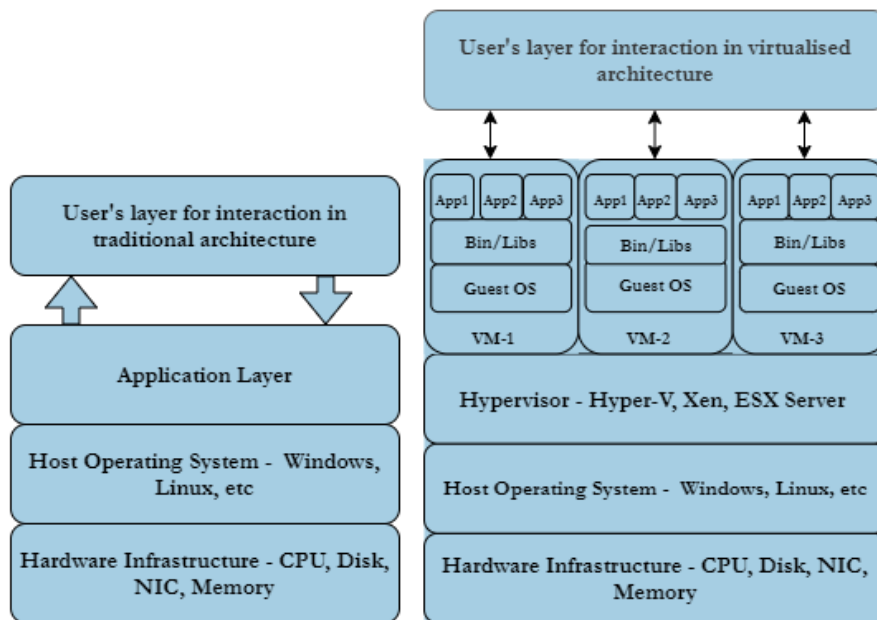


Figure 10. Hybrid Computing Stacks.

Emulation replicates the operations within the target infrastructure through a mirror system, while simulation replicates the behaviour of the target system through a model; thus, simulation is preferred in virtual training applications.

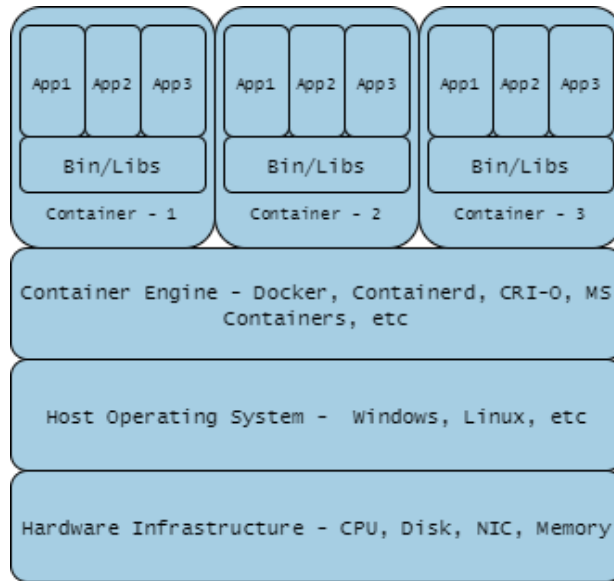


Figure 11. Containerisation Technology.

4.2.2. Infrastructure Technologies

Technologies that establish, manage, and control CRs are located between the core and front-end layers (Figure 8). Their selection vary widely based on CR developers’ preference and the goal application of the CR. The range of technologies are readily available, example being virtualisation management solutions such as vSphere and Wisper.

A number of CR implementations [17,24] utilise a combination of physical servers with virtual solutions. In these cases, the physical server has direct and exclusive access to the physical hardware, and the virtualisation has virtual hardware emulated by the hypervisor, which in turn controls all access to the underlying physical hardware. Virtualisation acts as a layer in between the hardware and the host operating system. Two types of hypervisor are in routine use, referred to as Type 1 and Type 2. Type 1 hypervisor runs directly on the host machine’s physical hardware, while Type 2—more commonly known as a hosted hypervisor—is installed on top of an existing operating system. A hypervisor employs four main virtual resources; vCPU, vMemory, vNetwork (vSwitch), and vDisk.

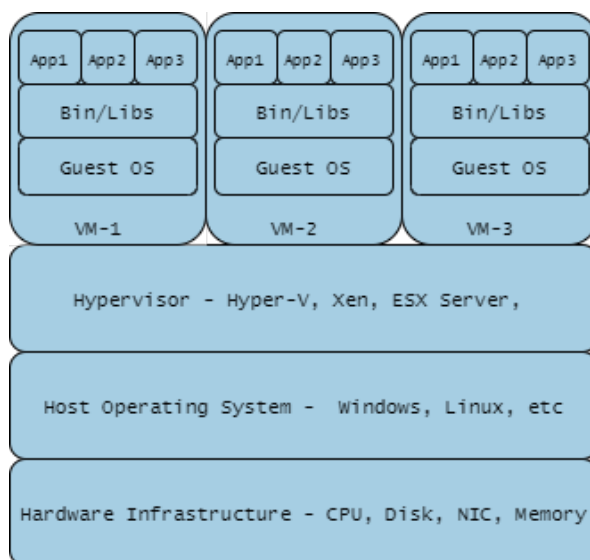


Figure 12. Virtualisation Technology.

SCADA-based TBs employ Human Machine Interfaces (HMI) server software, software-based Relay Terminal Units (RTUs) and Relay Programmers, as a consequence of the need to reproduce an exact model of the inter-dependencies between components. Accuracy of the model is essential in the evaluation of the effectiveness of cyber-attacks and their corresponding countermeasures [45,46].

Since many CR articles do not reveal the underlying infrastructural technology in use, e.g., vSphere, Wisper in their design and implementation, the use of ‘Available’ in the Table 2 indicates an infrastructure technology in use that cannot be specified, while ‘Not Available’ indicates that no information on the infrastructure technology was reported. Both are included for completeness.

4.2.3. Front-End Technologies

The bridge between end user and the CR—Core and Infrastructure—is the Front-End; the Core, infrastructure and user type determine the features of the Front-End. The basic elements of a web server as shown in Figure 13 represent the Hardware and Software components, the former is the physical server used by the hosting providers and the latter comprises an operating system and Hyper-Text Transfer Protocol (HTTP) server databases and scripting languages that enhance the capabilities of the web server. A Web server such as Apache or Nginx is deployed at the back-end coupled with a Content Management System (CMS) compiling results from scripting languages, databases, and HTML files to generate content for to the user. Web technologies provide the front-end interface as shown in Figure 8 such as HTML5-based console simulators.

TBs, on the other hand, rarely use front-end technologies as the environments being modelled are predominately Operational and Information Technology (OT/IT) systems on Human Machine Interface (HMI) servers, Historians, Software-based Remote Terminal Units (RTUs) and Relay Programmers [45]. Table 2 provides an overview of the available literature on CR Core, Infrastructure and Front-end technologies. In the same vein, Table 3 are the characteristics of two different types of available Test-Beds.

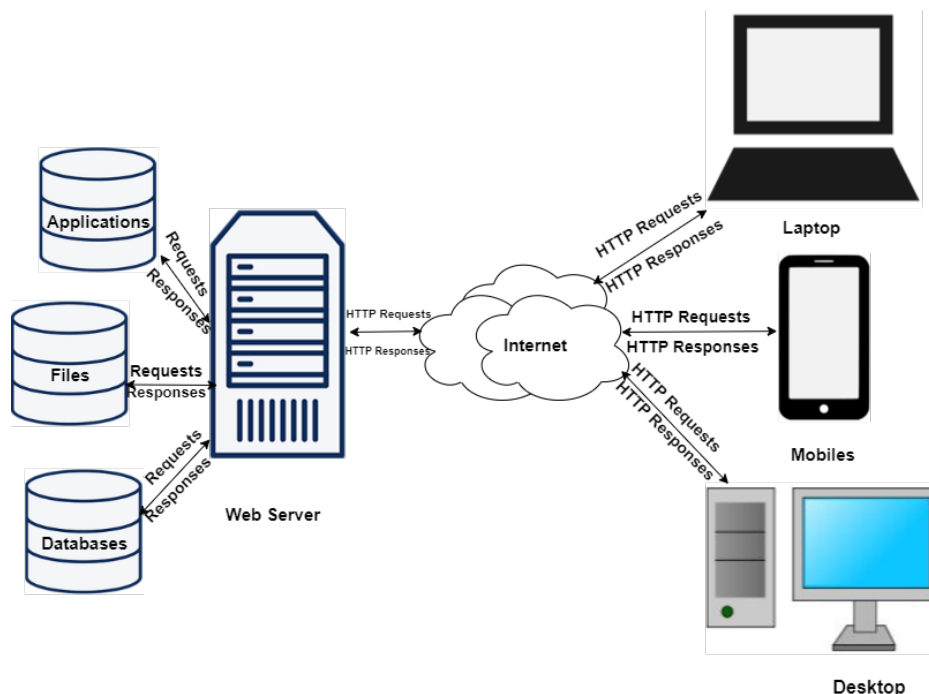


Figure 13. A Simple Web Server Architecture.

Table 2. CR and TB Technologies.

ine Classification	Ref.	Year	Core Technology	Infrastructure Technology	Front-End Technology
ine Cyber-SHIP	[47]	2019	Live Scenario	Not Available	Not Available
ine ICSRRange	[9]	2019	Simulation	Not Available	Not Available
ine Clusus	[48]	2019	Simulation	Available	Available
ine Testbed@TWISC	[40]	2018	Emulation	Available	Available
ine CYRAN	[49]	2018	Hybrid	Available	Available
ine INSALATA	[41]	2017	Emulation	Available	Available
ine Virginia CR	[21]	2017	Simulation	Available	Available
ine CyberVan	[42]	2016	Simulation	Available	Available
ine SoftGrid	[43]	2016	Emulation	Available	Available
ine SCADA-SST	[50]	2016	Simulation	Available	Available
ine KYPO	[51,52]	2015	Simulation	Available	Available
ine CRATE	[22]	2015	Emulation	Available	Available
ine DoD CR	[24]	2014	Simulation	Available	Available
ine SCADA-VT-A	[53]	2013	Live Scenario	Available	Available
ine StealthNet	[27]	2011	Simulation	Available	Available
ine NCR (DARPA)	[17,24]	2011	Emulation	Available	Available
ine PowerCyber	[45]	2010	Simulation	Available	Available
ine Reassure	[38]	2009	Simulation	Available	Available
ine ATC	[39]	2008	Live Scenario	Not Available	Not Available
ine CAAJED	[25]	2008	Simulation	Available	Available
ine DETER	[54]	2006	Emulation	Available	Available
ine RINSE	[29]	2005	Simulation	Not Available	Not Available
ine ViSe	[55]	2005	Emulation	Available	Available
ine NetENGINE	[30]	2003	Simulation	Available	Available
ine LARIAT	[33]	2002	Hybrid	Available	Available
ine					

Table 3. Offline and Real-Time Test-Beds.

Real-Time	Offline
Expensive	Less expensive
Complex	Easy implementation
Time-gain	Extended time
Integrate generators controllers	Cannot integrate hardware systems

5. Scenarios and Applications

Different scenarios and application areas of CRs and TBs technologies will be the focus of this section.

5.1. CRs and TBs Scenarios

Scenarios are simulated or emulated networks comprising traffic as well as potential threats in the network layer (PAN, LAN, MAN, WAN), software and hardware implemented through virtual machines (VMs), Containers or Sandboxes. In a bid to comprehensively represent target networks, the scenario can also feature other system peripherals and appliances. The simulated network environment is injected with traffic representative of user activities e.g., web surfing, email, and other server communications and real-life attack scenarios such as in Control or Data centres (Figure 14) are deployed. A predefined attack scenario library as well as custom-built scenarios are integral to the platform.

Yamin et al. [20] state that scenarios consist of Purpose, Environment, Storyline, Type, Domain and Tools, features to appropriately classifying a scenario aligned with the objectives of the exercise/training. The major differences between TB and CR scenarios are in the attack scenarios being simulated or emulated (Figure 14). TBs predominately simulate attacks in critical infrastructures such as energy sub-stations e.g., re-configuring a relay systems/devices Denial of Service (DoS), modifying/disrupting valid alarms, producing fake alarms, sending incorrect commands to the relay, manipulating readings from a relay, and injecting incorrect data to historian [45], whilst CRs most

often simulate multi-connected network such as Control Centres, Data Centres, and Internet-enabled IT/OT system attacks e.g., SQL Injection, Apache Shutdown, Web Defacement, Trojan Data Leakage, Java Network Monitoring System (NMS) Kill, Database (DB) Dump via File Transfer Protocol, Ransomware, DDoS, Synchronise (SYN) Flood, SCADA Human Machine Interface (HMI).

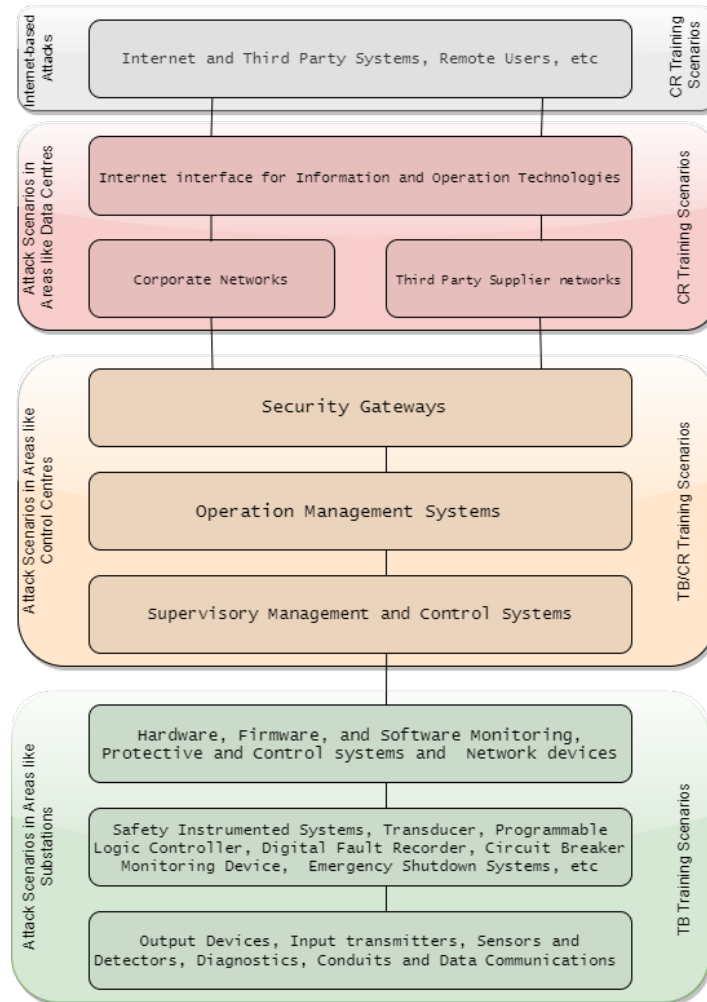


Figure 14. Attack scenarios types.

Scenarios depend largely on the application and the architecture of the network and adapt to the training goals. The relationship between the goals of the training and the optimum scenario remains fundamental in the assessment of the positive value of CR or TB.

Table 4 presents a list of attacks and their associated settings in the last five years. Attacks are classified by scenario complexity and type; ‘Low’ for scenarios with at least one attack test; ‘Medium’ for scenarios with two classical attacks; and ‘High’ for sophisticated or more than two attacks.

Scenario Design, Validation and Deployment

- Design: The definition of functional and non-functional as well as user and team-related requirements are essential pre-requisites in the design of a CR scenario. While the functional requirements pertain to the services the system provides, non-functional requirements describe how the system reacts to inputs and its dynamic responses. The team-related requirements are the tools and resources inherent within the exercise for use by teams [56]. Furthermore, ab initio a set of attack trees based on an understanding of how an attacker can gain access to the domain under

study is imperative to an effective attack scenario design. Thus a comprehensive vulnerability assessment must be established, and coupled with the impact scenarios, are combined produce a set of attack trees, the foundation for establishing a representative real-life breach condition and in turn enabling an evaluation of the optimum countermeasures to arrest the attack [45,57].

- **Validation:** Russo et al. [58] report on a framework for automating model validation of scenarios through a Scenario Definition Language (SDL) on the OASIS Topology and Orchestration Specification for Cloud Application (TOSCA) [59]. SDL/TOSCA based implementations automate the validation of the scenario against specified design errors, such as incorrect hardware/software bindings. The approach translates a SDL design into a Data Log specification, before verifying if the specification satisfies the goals of the scenario. A design modification is triggered whenever the validation fails, otherwise the scenario is automatically deployed. While developed for CR applications, the solution is also applicable to TBs but is dependent on the domain of study, most relevant in attack scenarios in targeting Control Centres (Figure 14).
- **Deployment:** A number of other approaches to activating scenarios have been reported. CRACK [60] are a SDL/TOSCA scenario definition, design and deployment languages and Automated Deployment of Laboratory Environments Systems (ADLES) [61], an open source specification language and associated deployment tool, achieve the same goals. ADLES provides an instructor a tool-set to design, specify, and semi-automatically deploy the training scenario together with tutorials as well as competitions. Furthermore, efficient sharing of classes together with the associated computing environment are provisioned to participants. The ADLES deployment begins with the verification and fixing of Master instances by converting them into templates followed by the use of these instances to clone services, create virtual networks and folders. The full exercise scenario on the specified virtualisation platform is then deployed. While these implementations are current state-of-art deployments, it is important to acknowledge that within the foreseeable future, the effectiveness of these tools will be diluted as the sophistication and complexity of cyber-attacks evolve powered through AI-based and Bio-Inspired attack strategies, motivating the need to migrate to Real-Time Auto-configurable systems.

5.2. CR and TB Applications

Figure 14 illustrates a clear trend in the convergence of CRs/TBs cyber-awareness training. While it is acknowledged that CRs cover a broader applications than TBs in the recent past, a number of domains where CRs are in particular use is becoming more evident, such as in industries for commercial purposes, education and research for academic purposes, military, defence and intelligence and in the defence of critical national infrastructure. TBs, although in use within these domains, are applied more extensively in Smart Grids and IoT architecture due to the embedded nature of HMI, Historian, RTUs, Relays implementations which better define the type of attack scenarios witnessed in these specific domains.

- **Industrial and Commercial:** IBM X-Force Command Centre [19] is the first commercial malware simulator that tests for the security of systems. At the heart of the simulator is a mobile Command Cyber Tactical Operations Center (C-TOC) that provides cyber-range and watch floor services. The C-TOC can be configured both as an immersive training CR, a platform for Red teaming and capture-the-flag competitions, as well as a watch floor for special security events. The Ixia Breaking Point, advertised as providing CR capabilities [16], is also a commercially available. The single rack-mountable appliance provides traffic generation and a ‘Strike Pack’ of network security and malware attacks. Exata is yet another commercially available simulation-based CR. A number of emulation-based CR are currently on offer, a good example being the ATC [39].
- **Education and Research:** Cohen [62] presents the development of SECUSIM [63], a highly customisable system with integrated Graphic User Interface (GUI) capabilities, the first example of the education and research community creating a training platform for simulating the impact

of attacks on computer networks [16]. The University of Illinois has developed the Real Time Immersive Network Simulation Environment (RINSE) in 2006, also primarily for training [29]. Other implementations in academia for modelling computer networks and intrusion detection systems (IDSs) attacks include the Virginia CR [21], Emulab [36], Virtualised CR [37], ARENA [31]. NetENGINE [30] has been designed for training on the strategies to combat cyber-attacks in large IP networks comprising a Virtual Cyber-Security Testing Capability (VCSTS) for the automated testing of new devices to assess its security robustness before deployment [34].

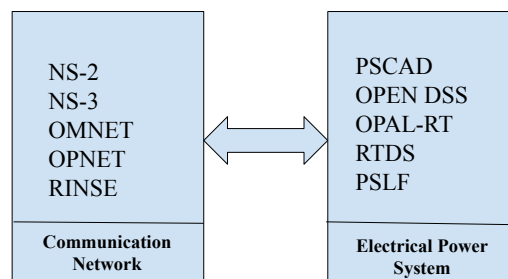
- **Military, Defence and Intelligence:** Davis and Magrath [16] assert that the USA Air Force (USAF) used CR around 2002, an element of the Simulator Training Exercise Network (SIMTEX) referred to as the Black Demon. The first reported CR was the Defence Advanced Research Projects Agency (DARPA)'s National Cyber Range (NCR) representing the foundation in the training of their military, defence and intelligence agencies on cyber warfare initiated by the United State military in 2009 as a consequence of the US Department of Defence classified military computer networking infrastructure being significantly compromised in 2008 [64]. Although NCR was largely a military-sponsored initiative, its use and application cut across the military, commercial, academic, and Government sectors [16,17]. Fourteen (14) CR applications in Military, Defense and Intelligence have been recorded to date ranging from CRATE [22], DoD CR [24], CAAJED [25], SAST [26], StealthNet [27], LARIAT [33] to INL [35]. Their role is not only to train the security agencies of sovereign countries on counter cyber-terrorism and warfare, but also to protect the nation's critical infrastructure such as Naval, Power and Aviation. SoftGrid [43] and CyberVan [42] are examples of TBs found in these application sectors.
- **Smart Grids:** The predominate area of application for TBs is Smart Grids owing to the reliance for the effective operation of an ever-evolving power network on an enabling communication network with information flow managing the power delivery. Consequently, the security of equipment and the critical signals that control the power system becomes essential for the safe, flexible and uninterrupted provision of the supply of energy.

A Smart Grid Test-bed can be cast as two simulation environments (Figure 15), one for the power, the other for the cyber/communication network. Co-simulator segmentation is a necessity as a hacker can target operations within both networks [12]. Here, TBs are classified into two categories; off-line and real-time. An off-line environment is the most prevalent approach realised, most readily, by SCADA systems [65]; refer to Table 3 for details. OMNET++ or NS2 are invariably at the core of most cyber simulators, with the TCP/IP protocol used to communicate between simulators. Synchronisation is central to the co-ordination of operations in the two domains. Real-time TBs have been proven to facilitate efficient training outcomes [66].

- **IoT Devices:** In the recent past, Internet-of-Things (IoT) architectures have evolved rapidly characterised by a growing complexity of inter-connections of an ever-increasing number of nodes ('things'). The proliferation of highly connected environments translates into an enhanced spectrum of vulnerabilities/opportunities for cyber criminals. Furthermore, IoT-inspired data-driven solutions have been adopted by key industry sectors as a means to implement business transformation. Securing network infrastructures consisting for example, of medical records, financial credential information against breaches becomes even more challenging. The training of security operators in these new classes of threats is essential. IoT Test-beds that can simulate different kinds of attacks play an important role in supporting the delivery of dynamically changing training requirements. Example IoT Test-Beds have been reported in [67–69].

Table 4. Some Cyber-Attacks and their Domain in the last 5 years.

Ref	Year	Domain	Tool	Complexity	Attack Type	Commentary
[70]	2020	Smart Grid	OPAL-RT	Medium	test-bed cyber events	Cyber attack needed to validate
[67]	2020	IoT	Open source platform	High	Extensive analysis/Automated tests	Time analysis needed to show the efficiency of Test-bed
[65]	2019	Smart Grid (PSCADA)	OMNET	Low	DoS/FDI	Lack of testes and scenarios
[71]	2019	IoT (SCADA)	–	Medium	DNS attack	security tests required
[72]	2019	IoT	QEMU emulator	Low	DDOS attack	Few attacks are tested
[73]	2018	Water storage (SCADA)	–	High	Packet injection/ARP spoofing/DoS	Real-time implementation discussion missed
[74]	2018	Information centric network	CONET	High	Input traffic pattern	Adding further experiences
[66]	2017	Smart Grid	OPAL-RT	High	Access to communication link	Real-time implementation of OPF model
[75]	2017	IoT	FIT/IoT LAB	Low	No attack tested	lack of security tests
[76]	2017	Cloud	Open source	Low	No attack tested	lack of security tests
[77]	2017	Industrial control system (SCADA)	–	Medium	Availability attack/Integrity attack	Detection tool should be implemented
[69]	2017	IoT(SCADA)	Hardware-based test bed	High	5 kinds of attack	Test bed with IDS
[78]	2016	IoT	Software-based OpenFlow switches	Low	No attacks	Software defined networking testbed
[79]	2016	Smart Grid	Real Time Digital Simulator	Low	Man-in-the-Middle attack	Test bed with Attack Resilient Control algorithm
[50]	2016	SCADA	C++	Low	Denial of Service attack	Test-bed based on SCADA simulation environment (SCADA-SST)
[80]	2016	SCADA	–	Low	Man-in-the-Middle Attack	Test-bed using CPS topology
[81]	2016	Power System	Real Time Digital Simulator (RTDS)	Medium	Aurora Attack/Network Based Cyber-Attacks	WAMS cyber-physical test-bed
[82]	2015	Power System	Real Time Digital Simulator (RTDS)	Medium	Measurement attack/Control attacks	PowerCyber CPS security Test-bed

**Figure 15.** Co-Simulation Test-bed.

5.3. CR and TB Realisation

The flowchart in Figure 16 describes the steps in its realisation;

1. Evaluate the weaknesses in the infrastructure; the architecture of the local network, past attacks, and the current security strategy should be examined.
2. Map the basic solutions; e.g., a firewall or control of external devices.
3. Asses current security policies; to enhance the security level of an infrastructure.
4. Training by simulation of attack exercises and scenarios; the definition of an appropriate virtual TB for training should adopt the following steps;

Step 1

A classification of the infrastructure is an essential step in advance of the realisation of the TB. Validation tests on the infrastructure may are required for an accurate classification.

Step 2

The vulnerabilities of the infrastructure should be identified; the localisation of vulnerabilities is important in informing on the security deficiencies within the infrastructure.

Step 3

Selection of the most appropriate software dependent on the application domain and the infrastructure. As an example, in the Smart Grid environment, OPAL-RT can be chosen to simulate the electric power and a discrete event network simulator to simulate the communication network.

Step 4

A modular approach is adopted to describe the infrastructure, with the input/output of each module verified.

Step 5

A database of different tests and scenarios is created, fundamental for the validation of the TB.

Step 6

Users are trained to respond to a range of attacks and threat scenarios, with the relevant reports being extracted from the interface module of the TB.

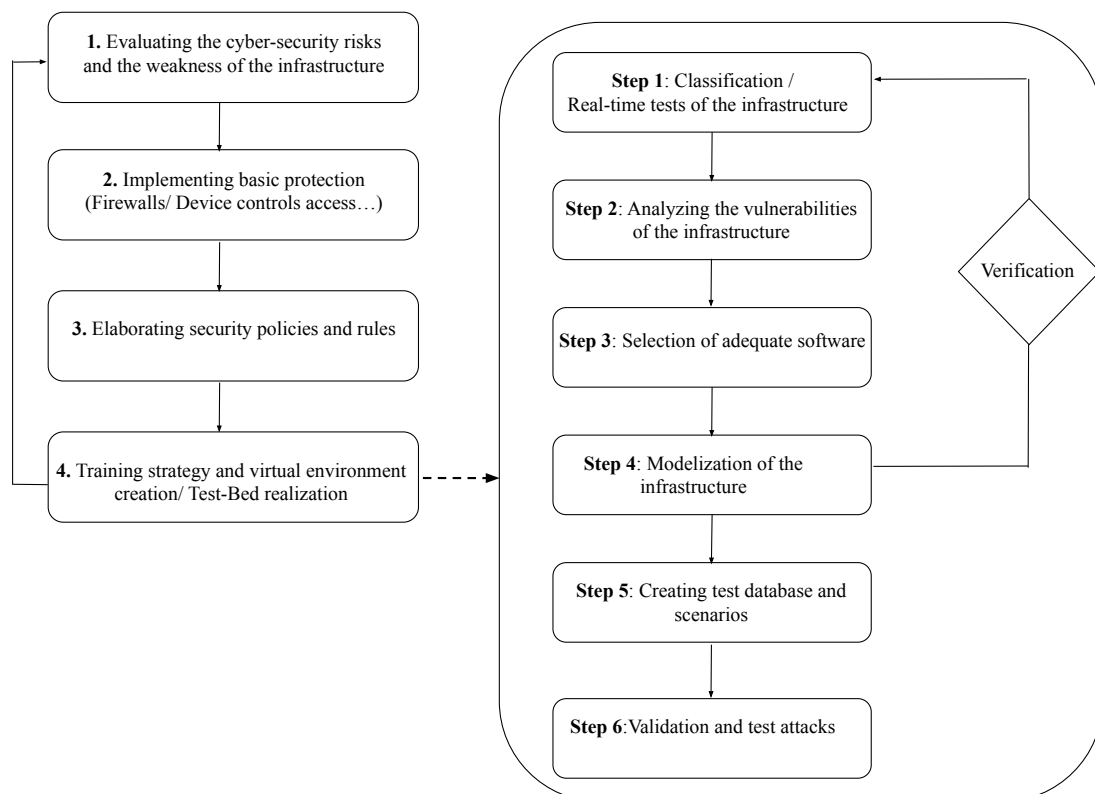


Figure 16. Cyber-range/Test-bed flowchart.

6. Analysis and Taxonomies

Two taxonomies in Figures 17 and 18 for treating CRs/TBs have been established based upon the reviewed literature. Current taxonomies encompass both CR and TB due to the close coupling between platforms, however, each offers different services governed by their implementation and training aims. The differentiation is captured in order to compile evidence demonstrating that CRs are mostly applied in IT while TB are preferred in OT environments. Moreover, CR are orientated towards end-users with a general understanding of the simulated architecture, while test-beds often require domain knowledge. The differentiation confirms the need for two separate taxonomies. In order to build the core of a CR, a scenario must be defined. The scenario must cover the following elements: (I) A narrative, enabling the user to evolve. (II) A domain of application, these domains can be broad or constrained (e.g., cyber training Vs maritime cyber training). (III) The education mechanics are core to the scenarios as they inform the platform mechanics during the scenario (i.e., collecting or displaying educational data for self reflection, case studies, etc.). (IV) These mechanisms further rely on the gamification. (V) The scenario can be of two types; dynamic or static.

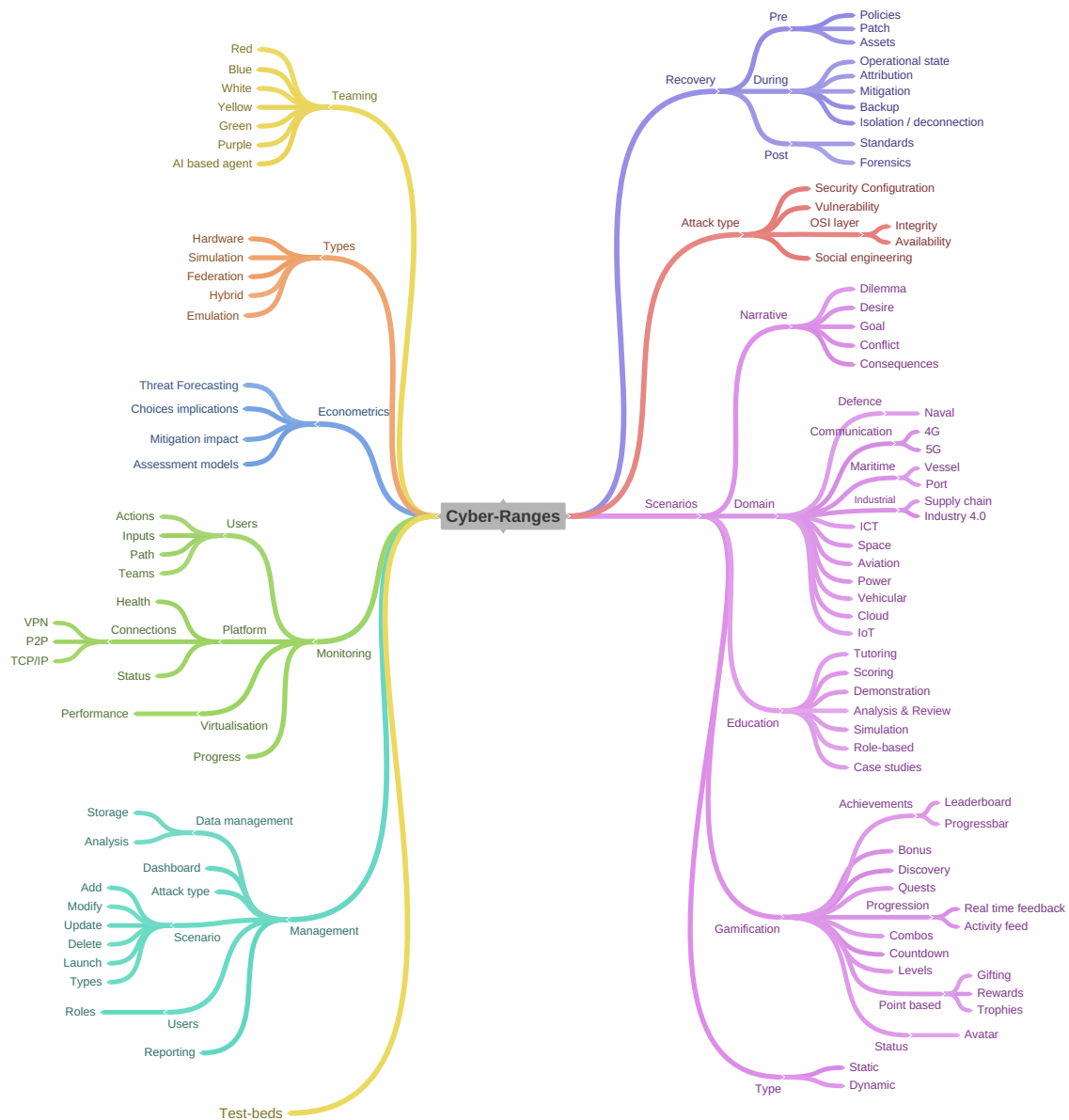


Figure 17. Cyber-Range Taxonomy.

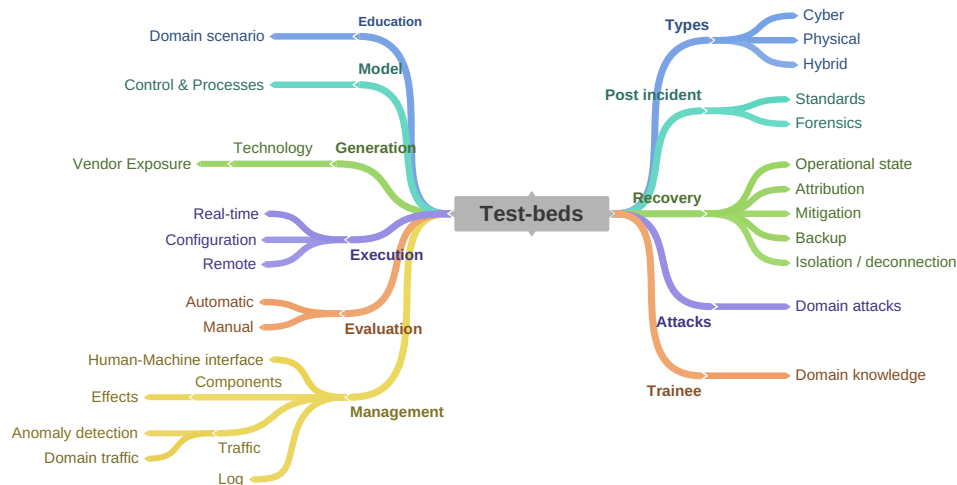


Figure 18. Test-Bed Taxonomy.

6.1. Cyber-Ranges

The definition of the cyber-range taxonomy is informed by future developments as inferred from the reviews conducted in this paper.

6.1.1. Management

The management layer presents a range of interfaces to various users, administering the collection, storage and analysis of the data describing scenarios and user-interactions. Information is presented to users through a dashboard along with the available scenarios and attack types per scenario. The layer also administers users and their roles as well as being responsible for reporting.

6.1.2. Monitoring

The component monitors users on the platform, capturing progress and assessing performance throughout the different scenarios as well as being responsible for connections of remote users to the platform, their actions, inputs paths selection and team formations. This component also validates the health of the platform and the various services and scenarios provisioned.

6.1.3. Econometrics

Understanding the impact of the actions taken by an user is essential, especially to estimate the level of situational awareness. The component executes an evaluation of the economic impact of actions taken by users within the various scenarios.

6.1.4. Types

Hardware based CRs allow training on operational technologies such as programmable logic controllers. Simulation/Emulation based CRs allow an infrastructure to be replicated, are scalable and cost effective, however, it is often challenging to replicate architecture accurately due to software limitations. A federated approach may be adopted where multiple CRs are clustered, each CR dedicated to simulating a single environment e.g., Large Enterprise Network and a Power Network and creating scenarios that span across all CRs. The hybrid solution, while similar, often depicts CRs composed of Hardware and Software solutions to provide both scalability, and affordability.

6.1.5. Teaming

Teams are at the heart of managing cyber protection services for organisations and consequently CRs are required to provide the appropriate environments for appropriate training. The Yellow team comprises application developers and software architects managing the CR. The *Green* team focuses on enhancing the security provision, the automation of tasks and ensure that the code is of the highest quality. The *Orange* team facilitates the education and is responsible of the creation and development of scenarios. The *Blue* team focuses on developing defensive actions, to protect the network and define the most effective countermeasure to arrest the breach. The *Red* team adopts an offensive stance, often competing against the Blue team. Finally, the *Purple* team is composed of users with both Blue and Red team skills, with knowledge of both defensive and offensive tactics.

6.1.6. Recovery

The recovery component ensures that all policies and patches remain up to date. The component maintains the operational state of the CR during an exercise, executes regular back-ups and restricts cyber-attacks spilling from the CR. The function is central for digital forensic purposes post incident/cyber-attack.

6.1.7. Attack Types

The component encompasses descriptions of the different attacks including the security configurations for the vulnerabilities within scenarios. A database of the vulnerabilities, as well as a high/low level description of each mapped against the OSI model is established.

6.1.8. Scenarios

The scenario component is subdivided in five sub-components focusing on (I) the Narrative—it is essential for a scenario to have a target goal as well as the consequences of any action. A desire, dilemma and conflicts can also be added to enrich the learning environment. (II) the Domain defines the context in which the scenario is currently being simulated. (III) the Education supports users to navigate and learn the skills necessary to complete the scenario through tutoring, scoring, demonstration, analysis and review of actions with the user in a role base fashion or through a specific case study. (IV) Gamification is used to embed game mechanics to drive and maintain the level of user engagement e.g., encourage users to engage with the platform and/or to perform a specific task by enticing with a lure aligned to user behaviour/preferences. (V) the type of scenario can be either static with a single goal or dynamic evolving with each action of the user.

6.2. Test-Beds

In line with the CR taxonomy discussed earlier, the focus of the proposed TB taxonomy is also informed by future developments/technologies.

6.2.1. Education

The Education component is used to explore new security scenarios, most often utilised by the evaluation team to develop and confirm the scenario for the optimum learning outcomes best students. Such exercises may include the evaluation of the formative assessment and ease of implementation.

6.2.2. Model

The Modelling component provides control as well as directs process on the innovation cycle. A model of the innovation is created and processed in a controlled environment satisfying a set of constraints.

6.2.3. Generation

The Generation component provisions comprehensive information on the underlying technology and vendors, inputs that inform the features of the innovation and its deployment.

6.2.4. Execution

Real-time, configuration-based remote creation of innovation provide insights into its impact on the behaviours of the system being modelled or tested. Essential to the test of the resilience of the targeted system is an evaluation of the behaviour at different execution scenarios, optimally executed within a controlled environment as that provided by a test-bed.

6.2.5. Evaluation

Evaluation of model within a TB can be done manually or automatically. The former is executed with human intervention, the latter harnesses an algorithm established with considerations of the key variables of the system.

6.2.6. Management

The Management components like CRs, present a number of interfaces as a function of the type of users. The services ranging from managing human-machine interface between the user and the TB helping to mitigate the limitations of these interactions, to managing the traffic for anomaly detection and representative domain traffic. The module also provides log statistics of user activities, generates reports and feedback. For example, SCADA-based TBs employ Human Machine Interfaces server software, software-based Relay Terminal Units and Relay Programmers. An accurate model of the inter-dependencies between the energy and cyber components is essential to the evaluation of the impact of cyber-attacks and in informing on the most effective countermeasure.

6.2.7. Types

Cyber-based TBs test innovation in an Internet-enabled environment; stand-alone physical TBs operate within an controlled environment, isolated from an operational network. The hybrid TB solution is a combination of Cyber and Physical TBs, comprising hardware and software in a networked as well as an isolated environment to provide training in OT, scalability, and affordability.

6.2.8. Post-Incident

The component ensures the integrity of the post incident procedures, the basis for an investigation of the performance of an innovation as well as confirming the validity of the process used in testing an attack or a failure of an innovation. Standard and Forensics are two types of Post-Incidence investigation, the former used to provide a detailed review that helps to understand each phase of an incident, from start to finish. In a situation awareness review, such components are one step in the incident response process that requires a cross-functional participation from all individuals to determine the root cause and full scope of the attack. Forensic, on the other hand, enables a scientifically derived and proven method to collect, validate, identify, analyse and interpret evidence derived from digital sources. An evidence-based review that characterises an incident from start to finish is generated.

6.2.9. Recovery

Recovery ensures that all policies are up to date, that the operational state is maintained and that regular back-ups are being carried out. The component is also of use for digital forensic purposes after an incident, helping to mitigate further failure or attack. Furthermore, in the process of surfacing the root causes of failures, it helps in isolating and disconnecting the system under investigation.

6.2.10. Attacks

The Attack component encompasses descriptions of potential attacks including the security configurations for the vulnerabilities within scenarios. A database of the vulnerabilities is created together with a high/low level description of each vulnerability mapped against the OSI model.

6.2.11. Trainee

The Trainee component contains specific domain knowledge required for and records the progress of each trainee with regard to specific modules and performance measures. A report is usually displayed in the trainee dashboard.

7. Training Methods

The spine of the training is founded on strategies informed by educational methodologies and is most often segmented into two classes. The first is centred on the relationship between coach and trainee using classical training methods characterised by the use of a number of support tools such as online courses, certification, training, and presentation. The second method relies more heavily on new elements such as gamification and video-assisted techniques.

Classical Training: The fundamental goal is to train trainees to acquire new skills. In the cyber-security context, the theoretical background and knowledge of security terminologies is considered the minimum level of achievement. In general, the information flow between a coach and a trainee is one-way. For instance, online courses and presentations which, for example, describe the architecture of an infrastructure is such a case, the trainee being a passive information recipient.

Classical training methods adopt a three-prong approach to learning ranging from getting acquainted with facts, followed by logical tools for the organisation of facts, culminating in the ability to critically analyse and draw conclusions [83]. The methodology inculcates the ability to comprehend and take timely and appropriate actions in dealing with cyber-related malicious activities both at the technical and operator level. The resultant knowledge on the successes and failures inherent in cyber defence scenarios, is central to a comprehensive cyber situation awareness training program in both the public and private sectors [84].

Training Methods: Simulation environments implemented through CRs are one of principle routes to establishing realistic scenarios of target systems, facilitating training through a rich illustration of real-life security incidents and threats dynamics, thereby preparing and equipping operators in the selection of the most appropriate responses. The predominant training role of TBs is to emulate the impact of a range of attack scenarios and test the strategies to arrest such attacks. The trainee is able to modify the parameters of attacks, test the effectiveness of responses and extract an analysis from the output reports. The result is an assessment of the security level of the infrastructure as a function of different attack scenarios. TBs are the foundation of the practical elements of the overall training.

The commonly used strands of the training scope can be classified as:

- **Gamification:** Gamification has been adopted to make cyber-security training more engaging and motivating [85]. The principle is to enhance exercises through a compelling experience utilising graphics and play. The aim is to enrich the challenge, engagement, as well as motivating the trainees owing to increased levels of interaction. The concept of 'Attacker-centric Gamification' was introduced by Adams and Makramalla in [86] with the goal empowering trainees to assume the roles of attacker combining gamification with entrepreneurial perspectives with an emphasis on surfacing their abilities, skills, knowledge, motivation, and resources [87].
- **Mock Attack Training:** The training method, developed by Sadeh et al. [88], embodies an approach that senses user actions which expose that user's infrastructure to cyber threats. The action could be as a result of a mock attack delivered to the user through a messaging service from any device, a wireless communication service or a fake malware application. The system

selects the most appropriate training from a list of available training routines based on the users' reaction to the message in so doing delivering the most targeted training.

- **Role-Based Training:** One practical training approach through CR-enabled scenarios is to assign unique roles to trainees. Such roles, for example emulating or taking the place of a hacker in a real life situation, cyber offensive operator, cyber defender, or training instructor [89] can be dynamic depending on the exercise, defined or selected using databases that contain predefined roles. Furthermore, customisation to better emulate real-life enterprise is also possible.
- **Exercises:** Competitions such as [90–94], are aimed at developing problem solving techniques, proficiency, teamwork and cyber defense skills by providing the participants with sets of hands-on cyber-security exercises in real-world scenarios to the participants. 'Catch-The-Flag' is an example, a distributed, wide-area security hacking competition involving multiple teams. 'Cyber Defense Exercise (CDX)' is another form of such an exercise in a larger setting where an inter-agency academy of an institution competes in the design, implementation, management and defend a network of computers. CDX is established by setting objectives, selecting an approach, defining a network topology, creating a scenario, stipulating the rules and choosing the right metrics with which to determine the lessons learnt [95].

8. The Future of CRs and TBs

8.1. Future Trends

- **Real-Time Auto-configurable Systems:** MIT's Lincoln Laboratory developed an advanced tool for cyber-ranges referred to as Automatic Live Instantiation of a Virtual Environment (ALIVE), [96], a range application extension to LARIAT. ALIVE has the capability of ingesting configuration files from Common Cyber Event Registration (CCER) to automate the building out of Virtual Machines and networking infrastructure of the CR [97]. In addition to the capability to create virtual networks, it can also automate most of the system network build-outs, creating end hosts, routers, firewalls, and servers needed to support traffic generation. The host software packages and user accounts can also be installed.

The Cyber-Range Instantiation System (CyRIS), an open source tool for facilitating cyber-range creation [98], can execute efficient instantiation of cyber-ranges automatically. CyRIS automatically aids in the preparation and management of CRs using a pre-defined specification provided by the scenario managers or instructors. The tool contains both basic functions for establishing the infrastructure as well its security settings.

ALPACA [99] is one of the modern auto-configurable CR with the facility to set user-specified constraints to generate complex cyber-ranges. The core of the implementation are an AI planning engine, a database of vulnerabilities and machine specific configuration parameters with the ability to generate a VM that includes the sequences of vulnerabilities and exploits.

- **Smart, Mobile and Integrated Technologies:** Pharos [100], a TB for Mobile Cyber-Physical Systems, is aimed at supporting mobile cyber-physical system evaluation in live networks. It is a networked system of independent mobile devices with its fundamental building block based on Proteus (an autonomous mobile system with highly modular software and hardware), with the capability of relating with each other and with networks of embedded sensors and actuators. Push-button repeatability facilitating the recreation of the same scenarios multiple times is an important feature of the TB.

Cybertropolis [101] is aimed at breaking the paradigm of CRs and TBs by providing what is referred to as Cyber-electromagnetic (CEMA) range facilities, which merges the features of CRs and TBs to yield a hybrid type of cyber-security training system. Cybertropolis was developed as a one-of-kind cyber-range that can be used in the areas of industrial control systems, cyber-physical devices, IoT and wireless systems. The platform provides the ability to create a heterogeneous

network consisting of virtual Information and Communication Technology (ICT) systems with integrated live cyber-physical systems, live Radio Frequency (RF), and Internet of Things (IoT) systems into a virtual environment.

- **Training with Augmented Reality Technology:** Augmented Reality (AR) is increasingly viewed as an important dimension in learning in different domains and is being considered as another impactful technology in future CR and TB training. AR offers the possibility of interaction with different parts of the systems, in so doing enriching the training owing to enhanced visualisation. Augmented reality TB or CR create a new interactive experience able to modify the trainee view of the progression of attacks. AR solution also gates portable solutions, as an example, the attack reaction could be modelled anywhere without infrastructure dependence. The environment can be modified and the programmer can add new attack scenarios.

8.2. Future Technologies

- **5G/6G Technologies:** 5th and 6th Generation (5G, 6G) networks will transform services using mobile and wireless network infrastructures by provisioning connections with advantageous features ranging from low latency with high network bandwidth capability through to machine-to-machine communication. 5G solutions enable better services using Virtualisation and Cloud technologies [102], extending to Network Functions Virtualisation (NFV) which enhances server virtualisation to network devices. Tranoris et al. [102], utilised these capabilities to demonstrate real-time remote monitoring and video streaming between Vehicle-to-Vehicle (V2V) in an assisted overtaking application [103], showcasing the potential impact from emerging 5G and beyond. Mitra and Agrawal [104], described a highly futuristic connected society—“smart living”: Vehicle Ad-hoc Networks (VANET) cloud for network connected transport systems managing dynamic real-time traffic demands; and massive M2M communications. West [105] also added that the revolution will bring about IoT-enabled health services while Letaief et al. [106] postulate that 6G will bring about ubiquitous AI-based services. The self-same capabilities present leveraging opportunities for CR and TB engineers and users to provide a seamless, faster, and low latency-based CR and TB deployments using virtual machines, sandboxes or containerised technologies.
- **Containerisation Technologies:** The impact of hypervisor-enabled virtualisation technology in CRs/TBs cyber-warfare training has been highly beneficial. VMs provide the required isolation from operational networks but present users with real-life training scenarios. The deployment of applications to implement VMs on data centres needs a dedicated guest operating system on each VM, on occasion different from the host operating system. Containerisation technology has been introduced as light-weight virtualised technology to that of VMs in order to manage these concomitant accrued overheads. A study conducted by Bhardwaj and Krishna [107] compared the use of the pre-copy VM migration scheme with that of the LXD/CR container migration technique, concluding that the use of latter reduces system downtime by 76.66%, migration time by 65.55%, scalability (volume of data transferred) by 76.63%, throughput (number of transferred pages) by 76.78%, overhead costs were reduced with regards to CPU utilisation by 55.89% and RAM utilisation by 76.52%. Thus, containerised technology costs less, guarantees more system up-time and saves times. Other studies that highlight the benefits of containerised technologies are Lovas et al. [108], on their software container-based simulation platform in order to achieve scalability and portability; Mucci and Blumbers [109] to gain flexibility, reduce complexity while providing extensibility; and Kyriakou et al. [110], to ease deployment, management and resilience of their cloud-based environment.

8.3. Future Application Areas

- **Smart Cyber-Physical Systems:** Smart Cyber-Physical Systems (sCPS) are large-scale software intensive and pervasive systems, that are intelligent, self-aware, self-managing and

self-configuring [111]. In line with other data driven artificially intelligence powered systems, sCPS utilise multiple data streams to manage real-world processes efficiently and through these offers a broad range of new applications and services in housing, hospital, transportation and automobile applications.

In recent times, cyber-attackers have up-skilled their skills through AI techniques to automate attacks, augment their strategies, launch more sophisticated attacks and by implication increase the success rates [112,113]. ICT tools and AI techniques have not only enriched the opportunities for cyber-attackers as a new form of threat landscape has suddenly emerged. There is a pressing obligation for cyber-range based training to evolve as a consequence implementing the detection as well as informing on optimum mitigation of these new threat dynamics.

- **Smart Cities and Industry 4.0:** The 4th Industrial revolution, also referred to as Industry 4.0, are data driven, network connected, digitalised industrial systems, heralding an era of automated manufacturing and service delivery with strong potential of process optimisation, imbued with new business practices. The evolution is, however, not without its attendant new cyber-threats. CyberFactory#1 [114] is designed to proffer a solution between future digital factories and security threats gated by digitalisation. The principles on which the environment is established are conscious design, development, and demonstration of a System-of-Systems embracing the technical, economical, human and societal dimension of future factories [12]. The platform demonstrates sets of major enabling capabilities that foster optimisation and resilience of next generation manufacturing and service delivery industries. As the evolution unfolds, there is a need to continue to propose new solutions capable of mitigating the dilemma between the deployment of future factories/smart cities and cyber-threats.

A body of available literature stresses that cyber threats and privacy concerns will increase significantly in smart systems due to high degrees of network inter-connectivity; Reys et al. in [115], Baig et al. in [116], Vitunskaitė et al. in [117], Mylrea et al. in [118], Srivastava et al. in [119], Aldairi et al. in [120], Cerrudo et al. in [121], Alibasic et al. in [122] and Braun et al. in [123]. Wang et al. in [124] and Farahat et al. in [125] focused on data security as well as threat modeling for smart city infrastructures. Vattapparamban et al. in [126] expect that drones will be used in service delivery in highly connected smart cities environments of the future and hence will become a factor in defining the scope of cyber-attacks. Li et al. in [127] report on the intelligent management of network traffic to avoid congestion while reducing cyber-security concerns in Smart cities.

- **Aerospace and Satellite Industries:** The evolution of the aerospace and satellite industries and the significant contribution the sector makes to the health of the economy has made them a central interest for cyber-attacks. CRs and TBs are essential to model the impact of cyber-attack effects and enhance the ability of protecting this critical infrastructure. The goal is to understand and overcome the spectrum of possible attacks by taking into account the sensitivity of information used. Virtualisation using a simulation-based system is a potential solution to implement TBs, but a total recognition of several parts of such critical infrastructure should be studied. The prediction of the hacker's strategies and aims remain the core to understanding the optimum countermeasure against class of attack.

9. Conclusions

The rapid proliferation in the automation of cyber-attacks is diminishing the gap between information and operational technologies and in turn stimulating an increased reliance on training to inculcate robust cyber-hygiene knowledge for cyber-security professionals, trainers and researchers. Cyber-Situational awareness is now viewed as a central spine in the effective provision of practices that protect organisations/infrastructures against a cohort of more sophisticated cyber-attackers. From necessity, the training must be delivered through non-operational environments that provide

real-time information on cyber-threats, their early identification/characterisation and effective countermeasures. This paper presents an evaluation of prominent CR and TB platforms segmented by type, technology, threat scenarios, applications and the scope of attainable training. Furthermore, a novel taxonomy for CRs and TBs is presented which represents the foundation for the prediction of the evolution of CRs/TBs. In all, this automation has accentuated a rapidly diminishing differentiation between CRs and TBs respective areas of application.

Author Contributions: Conceptualization and formal analysis, E.U., M.A.B.F., H.H. and X.B.; investigation, E.U., M.A.B.F. and H.H.; methodology, E.U., M.A.B.F., H.H., I.A. and X.B.; validation, E.U., M.A.B.F., D.B., D.K., R.A., C.T., M.B., I.A. and X.B.; writing—original draft preparation, E.U., M.A.B.F. and H.H.; and writing—review and editing, E.U., M.A.B.F., D.B., D.K., R.A., C.T., M.B., I.A. and X.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research is supported by the European Union Horizon 2020 Programme under Grant Agreement No. 833673. The content reflects the authors' view only and the Agency is not responsible for any use that may be made of the information within the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Denning, D.E. Stuxnet: What has changed? *Future Internet* **2012**, *4*, 672–687. [CrossRef]
- Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *arXiv* **2020**, arXiv:cs.CR/2006.11929.
- Leyden, J. *Stuxnet' a Game Changer for Malware Defence'*; The Register: London, UK, 2010.
- Mitchell, R. After Stuxnet: The new rules of cyberwar. *Computerworld* **2012**, *5*, 1.
- Benson, P. Computer Virus Stuxnet a 'Game Changer', DHS official tells Senate. Available online: <http://edition.cnn.com/2010/TECH/web/11/17/stuxnet.virus/index.html> (accessed on 11 December 2020).
- Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia, 4–7 December 2018; pp. 62–68.
- Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *J. Comput. Inf. Syst.* **2020**, 1–16. [CrossRef]
- Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Spec. Publ.* **2017**, *800*, 181.
- Giuliano, V.; Formicola, V. ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems. *arXiv* **2019**, arXiv:1909.01910.
- Yonemura, K.; Sato, J.; Komura, R.; Matsuoka, M. Practical security education on combination of OT and ICT using gamification method. In Proceedings of the 2018 IEEE Global Engineering Education Conference (EDUCON 2018), Tenerife, Spain, 17–20 April 2018; pp. 746–750.
- Van der Velde, D.; Henze, M.; Kathmann, P.; Wassermann, E.; Andres, M.; Bracht, D.; Ernst, R.; Hallak, G.; Klaer, B.; Linnartz, P.; et al. Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures. *arXiv* **2020**, arXiv:2003.06185.
- Vozikis, D.; Darra, E.; Kuusk, T.; Kavallieros, D.; Reintam, A.; Bellekens, X. On the Importance of Cyber-Security Training for Multi-Vector Energy Distribution System Operators. In Proceedings of the 15th International Conference on Availability, Reliability and Security, online, 25–28 August 2020. [CrossRef]
- Okoli, C.; Schabram, K. A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electron. J.* **2010**. [CrossRef]
- Okoli, C. A Guide to Conducting a Standalone Systematic Literature Review. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 43. [CrossRef]
- Bures, M.; Klima, M.; Rechtberger, V.; Bellekens, X.; Tachtatzis, C.; Atkinson, R.; Ahmed, B.S. Interoperability and Integration Testing Methods for IoT Systems: A Systematic Mapping Study. In *Software Engineering and Formal Methods*; de Boer, F., Cerone, A., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 93–112.

16. Davis, J.; Magrath, S. A Survey of Cyber Ranges and Testbeds. Available online: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a594524.pdf> (accessed on 11 December 2020).
17. Ranka, J. National Cyber Range. Available online: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a551864.pdf> (accessed on 11 December 2020).
18. Leblanc, S.P.; Partington, A.; Chapman, I.M.; Bernier, M. An Overview of Cyber Attack and Computer Network Operations Simulation. In Proceedings of the 2011 Military Modeling & Simulation Symposium, Boston, MA, USA, 3–7 April 2011; pp. 92–100.
19. Priyadarshini, I. Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey. Ph.D. Thesis, University of Delaware, Newark, DE, USA, 2018.
20. Yamin, M.M.; Katt, B.; Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Comput. Secur.* **2020**, *88*, 101636. [CrossRef]
21. Radziwill, N.M. Virginia cyber range. *Softw. Qual. Prof.* **2017**, *19*, 46.
22. Sommestad, T. Experimentation on Operational Cyber Security in CRATE. Available online: <http://www.sommestad.com/teodor/Filer/Sommestad%20-%202015%20-%20Experimentation%20on%20operational%20cyber%20security%20in%20CRATE.pdf> (accessed on 11 December 2020).
23. Pernik, P. Improving Cyber Security: NATO and the EU. Available online: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf (accessed on 11 December 2020).
24. Ferguson, B.; Tall, A.; Olsen, D. National cyber range overview. In Proceedings of the 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014; pp. 123–128.
25. Mudge, R.S.; Lingley, S. Cyber and Air Joint Effects Demonstration (CAAJED). Available online: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.476&rep=rep1&type=pdf> (accessed on 11 December 2020).
26. Meitzler, W.D.; Ouderkirk, S.J.; Hughes, C.O. *Security Assessment Simulation Toolkit (SAST) Final Report*; Technical report; Pacific Northwest National Lab.: Richland, WA, USA, 2009.
27. Varshney, M.; Pickett, K.; Bagrodia, R. A live-virtual-constructive (LVC) framework for cyber operations test, evaluation and training. In Proceedings of the 2011-MILCOM 2011 Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011; pp. 1387–1392.
28. Chi, S.D.; Park, J.S.; Lee, J.S. A role of DEVS simulation for information assurance. In *International Workshop on Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 27–41.
29. Liljenstam, M.; Liu, J.; Nicol, D.; Yuan, Y.; Yan, G.; Grier, C. Rinse: The real-time immersive network simulation environment for network security exercises. In Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS'05), Monterey, CA, USA, 1–3 June 2005; pp. 119–128.
30. Brown, B.; Cutts, A.; McGrath, D.; Nicol, D.M.; Smith, T.P.; Tofel, B. Simulation of cyber attacks with applications in homeland defense training. In Proceedings of the Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement II, Orlando, FL, USA, 21–25 April 2003; pp. 63–71.
31. Kuhl, M.E.; Sudit, M.; Kistner, J.; Costantini, K. Cyber attack modeling and simulation for network security analysis. In Proceedings of the 2007 Winter Simulation Conference, Washington, DC, USA, 9–12 December 2007; pp. 1180–1188.
32. Zhou, M.; Lang, S.D. A Frequency-Based Approach to Intrusion Detection. Available online: https://d1wqtxts1xzle7.cloudfront.net/56628641/dosdos.pdf?1527000071=&response-content-disposition=inline%3B+filename%3DA_Frequency_Based_Approach_to_Intrusion.pdf&Expires=1607693224&Signature=BsARTy9SFcwtmh3em1-GabLEdtohfiBZqLiuH5ODCyL5hife4Ga95~urso2IqlZxQnaAN~GepEHt8ovbOD9-XdAXMfLvKQ6PCBdFX5fhWYE2ZOGWfgcBjEy16pMT9egqXlZkSr4e-raPjDQy6GxeQRTTe4Z~tIQTctdI6dn6GOGQssPh3lv5bwwbi6CnPBScFCv823Gwfbk2rPp5WyLGRMKFaXlqRdzmFrqYKdUpsTeRK-bNXBjViTrD6hlbA0iF13ELVh431TX1OC1elbrdZWaQL8sZPmi6YmM5XNH2SJ5RyqawQ1HrHjA9-Jhs3kMs5rqRw9l857KsGg9G4Whwg_&Key-Pair-Id=APKAJLOHF5CGSLRBV4ZA (accessed on 11 December 2020).
33. Rossey, L.M.; Cunningham, R.K.; Fried, D.J.; Rabek, J.C.; Lippmann, R.P.; Haines, J.W.; Zissman, M.A. LARIAT: Lincoln adaptable real-time information assurance testbed. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 9–16 March 2002; p. 6.
34. Pederson, P.; Lee, D.; Shu, G.; Chen, D.; Liu, Z.; Li, N.; Sang, L. Virtual Cyber-Security Testing Capability for Large Scale Distributed Information Infrastructure Protection. In Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA, 12–13 May 2008; pp. 372–377.

35. Anderson, R.S. *Cyber Security and Resilient Systems*; Technical report; Idaho National Laboratory: Idaho Falls, ID, USA, 2009.
36. Siaterlis, C.; Garcia, A.P.; Genge, B. On the use of Emulab testbeds for scientifically rigorous experiments. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 929–942. [CrossRef]
37. Mayo, J.; Minnich, R.; Rudish, D.; Armstrong, R. Approaches for Scalable Modeling and Emulation of Cyber Systems: LDRD Final Report. Available online: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.1793&rep=rep1&type=pdf> (accessed on 11 December 2020).
38. Thomas, J.; Meunier, P.; Eugster, P.; Vitek, J. Mandatory access control for experiments with malware. In Proceedings of the 10th Annual Information Security Symposium, West Lafayette, IN, USA, 9–10 April 2009.
39. Brueckner, S.; Guaspari, D.; Adelstein, F.; Weeks, J. Automated computer forensics training in a virtualized environment. *Digit. Investig.* **2008**, *5*, S105–S111. [CrossRef]
40. Tsai, P.W.; Yang, C.S. Testbed@TWISC: A network security experiment platform. *Int. J. Commun. Syst.* **2018**, *31*, e3446. [CrossRef]
41. Herold, N.; Wachs, M.; Dorfhuber, M.; Rudolf, C.; Liebold, S.; Carle, G. Achieving reproducible network environments with INSALATA. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*; Springer: Cham, Switzerland, 2017; pp. 30–44.
42. Chadha, R.; Bowen, T.; Chiang, C.Y.J.; Gottlieb, Y.M.; Poylisher, A.; Sapello, A.; Serban, C.; Sugrim, S.; Walther, G.; Marvel, L.M.; et al. Cybervan: A cyber security virtual assured network testbed. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 1125–1130.
43. Gunathilaka, P.; Mashima, D.; Chen, B. Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Vienna, Austria, 28 October 2016; pp. 113–124.
44. Haines, J.W.; Rossey, L.M.; Lippmann, R.P.; Cunningham, R.K. Extending the darpa off-line intrusion detection evaluations. In Proceedings of the DARPA Information Survivability Conference and Exposition II. DISCEX'01, Anaheim, CA, USA, 12–16 June 2001; pp. 35–45.
45. Hahn, A.; Kregel, B.; Govindarasu, M.; Fitzpatrick, J.; Adnan, R.; Sridhar, S.; Higdon, M. Development of the PowerCyber SCADA security testbed. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 21–23 April 2010; pp. 1–4.
46. Hindy, H.; Brosset, D.; Bayne, E.; Seem, A.; Bellekens, X. Improving SIEM for Critical SCADA Water Infrastructures Using Machine Learning. In *Computer Security*; Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinouidakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 3–19.
47. Tam, K.; Jones, K. Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities. Available online: <https://pearl.plymouth.ac.uk/handle/10026.1/14949> (accessed on 11 December 2020).
48. Hildebrand, E.; Flinterman, R.; Mulder, J.; Smit, A. Clusus: A Cyber Range for Network Attack Simulations. Available online: <http://resolver.tudelft.nl/uuid:2588ee53-0249-476f-aa53-54d7a368dc8e> (accessed on 11 December 2020).
49. Hallaq, B.; Nicholson, A.; Smith, R.; Maglaras, L.; Janicke, H.; Jones, K. CYRAN: A hybrid cyber range for testing security on ICS/SCADA systems. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2018; pp. 622–637.
50. Ghaleb, A.; Zhioua, S.; Almulhem, A. SCADA-SST: A SCADA security testbed. In Proceedings of the 2016 World Congress on Industrial Control Systems Security (WCICSS), London, UK, 12–14 December 2016; pp. 1–6.
51. Čeleda, P.; Čegan, J.; Vykopal, J.; Tovarňák, D. Kypo—A platform for cyber defence exercises. Available online: <https://is.muni.cz/repo/1319597/2015-NATO-MSG-133-kypo-platform-cyber-defence-exercises-paper.pdf> (accessed on 11 December 2020).
52. Vykopal, J.; Ošlejšek, R.; Čeleda, P.; Vizvary, M.; Tovarňák, D. Kypo Cyber Range: Design and Use Cases. Available online: <https://repozitar.cz/repo/26486/> (accessed on 11 December 2020).
53. Almalawi, A.; Tari, Z.; Khalil, I.; Fahad, A. SCADA-VT-A framework for SCADA security testbed based on virtualization technology. In Proceedings of the 38th Annual IEEE Conference on Local Computer Networks, Sydney, Australia, 21–24 October 2013; pp. 639–646.

54. Benzel, T.; Braden, R.; Kim, D.; Neuman, C.; Joseph, A.; Sklower, K.; Ostrenga, R.; Schwab, S. Experience with deter: A testbed for security research. In Proceedings of the 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM, Barcelona, Spain, 1–3 March 2006.
55. Richmond, M. ViSe: A virtual security testbed. Available online: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.2205&rep=rep1&type=pdf> (accessed on 11 December 2020).
56. Marrocco, D. Design and Deployment of a Virtual Environment to Emulate a Scada Network within Cyber Ranges. Ph.D. Thesis, Politecnico di Torino, Torino, Italy, 2018.
57. Ten, C.W.; Liu, C.C.; Govindarasu, M. Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In Proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 24–28 June 2007; pp. 1–8.
58. Russo, E.; Costa, G.; Armando, A. Scenario design and validation for next generation cyber ranges. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–4.
59. Binz, T.; Breitenbücher, U.; Kopp, O.; Leymann, F. TOSCA: Portable automated deployment and management of cloud applications. In *Advanced Web Services*; Springer: New York, NY, USA, 2014; pp. 527–549.
60. Russo, E.; Costa, G.; Armando, A. Building Next Generation Cyber Ranges with CRACK. *Comput. Secur.* **2020**, *95*, 101837. [[CrossRef](#)]
61. De Leon, D.C.; Goes, C.E.; Haney, M.A.; Krings, A.W. ADLES: Specifying, deploying, and sharing hands-on cyber-exercises. *Comput. Secur.* **2018**, *74*, 12–40. [[CrossRef](#)]
62. Cohen, F. Simulating cyber attacks, defences, and consequences. *Comput. Secur.* **1999**, *18*, 479–518. [[CrossRef](#)]
63. Park, J.S.; Lee, J.S.; Kim, H.K.; Jeong, J.R.; Yeom, D.B.; Chi, S.D. Secusim: A tool for the cyber-attack simulation. In Proceedings of the International Conference on Information and Communications Security, Xi'an, China, 13–16 November 2001; pp. 471–475.
64. Lynn, W.F., III. Defending a new domain—the Pentagon's cyberstrategy. *Foreign Aff.* **2010**, *89*, 97.
65. Hammad, E.; Ezeme, M.; Farraj, A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 817–826. [[CrossRef](#)]
66. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [[CrossRef](#)]
67. Waraga, O.A.; Bettayeb, M.; Nasir, Q.; Talib, M.A. Design and implementation of automated IoT security testbed. *Comput. Secur.* **2020**, *88*, 101648. [[CrossRef](#)]
68. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A software-defined security framework for IoT environments. *Comput. Netw.* **2019**, *163*, 106889. [[CrossRef](#)]
69. Lee, S.; Lee, S.; Yoo, H.; Kwon, S.; Shon, T. Design and implementation of cybersecurity testbed for industrial IoT systems. *J. Supercomput.* **2018**, *74*, 4506–4520. [[CrossRef](#)]
70. Wang, Y.; Nguyen, T.L.; Xu, Y.; Shi, D. Distributed control of heterogeneous energy storage systems in islanded microgrids: Finite-time approach and cyber-physical implementation. *Int. J. Electr. Power Energy Syst.* **2020**, *119*, 105898. [[CrossRef](#)]
71. De La Torre, G.; Rad, P.; Choo, K.K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [[CrossRef](#)]
72. Kumar, A.; Lim, T.J. A Secure Contained Testbed for Analyzing IoT Botnets. In Proceedings of the International Conference on Testbeds and Research Infrastructures, Shanghai, China, 1–3 December 2018; pp. 124–137.
73. Alves, T.; Das, R.; Werth, A.; Morris, T. Virtualization of SCADA testbeds for cybersecurity research: A modular approach. *Comput. Secur.* **2018**, *77*, 531–546. [[CrossRef](#)]
74. Siracusano, G.; Salsano, S.; Ventre, P.L.; Detti, A.; Rashed, O.; Blefari-Melazzi, N. A framework for experimenting ICN over SDN solutions using physical and virtual testbeds. *Comput. Netw.* **2018**, *134*, 245–259. [[CrossRef](#)]
75. Papadopoulos, G.Z.; Gallais, A.; Schreiner, G.; Jou, E.; Noel, T. Thorough IoT testbed characterization: From proof-of-concept to repeatable experimentations. *Comput. Netw.* **2017**, *119*, 86–101. [[CrossRef](#)]
76. Liu, X.F.; Shahriar, M.R.; Al Sunny, S.N.; Leu, M.C.; Hu, L. Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed. *J. Manuf. Syst.* **2017**, *43*, 352–364. [[CrossRef](#)]

77. Bernieri, G.; Miciolino, E.E.; Pascucci, F.; Setola, R. Monitoring system reaction in cyber-physical testbed under cyber-attacks. *Comput. Electr. Eng.* **2017**, *59*, 86–98. [[CrossRef](#)]
78. Flauzac, O.; Gonzalez, C.; Nolot, F. Developing a distributed software defined networking testbed for IoT. *Procedia Comput. Sci.* **2016**, *83*, 680–684. [[CrossRef](#)]
79. Ashok, A.; Sridhar, S.; McKinnon, A.D.; Wang, P.; Govindarasu, M. Testbed-based performance evaluation of attack resilient control for AGC. In Proceedings of the 2016 Resilience Week (RWS), Chicago, IL, USA, 16–18 August 2016; pp. 125–129.
80. Deshmukh, P.P.; Patterson, C.D.; Baumann, W.T. A hands-on modular laboratory environment to foster learning in control system security. In Proceedings of the 2016 IEEE Frontiers in Education Conference (FIE), Erie, PA, USA, 12–15 October 2016; pp. 1–9.
81. Adhikari, U.; Morris, T.; Pan, S. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining. *IEEE Trans. Smart Grid* **2016**, *8*, 2744–2753. [[CrossRef](#)]
82. Ashok, A.; Wang, P.; Brown, M.; Govindarasu, M. Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed. In Proceedings of the 2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5.
83. Bauer, S.W. What Is Classical Education? Available online: http://www.bluegrasschristianacademy.org/wp-content/uploads/2015/06/Classical-Education_-_The-Well-Trained-Mind.pdf (accessed on 11 December 2020).
84. Brynielsson, J.; Franke, U.; Varga, S. Cyber situational awareness testing. In *Combating Cybercrime and Cyberterrorism*; Springer: Cham, Switzerland, 2016; pp. 209–233.
85. Boopathi, K.; Sreejith, S.; Bithin, A. Learning cyber security through gamification. *Indian J. Sci. Technol.* **2015**, *8*, 642–649. [[CrossRef](#)]
86. Adams, M.; Makramalla, M. Cybersecurity skills training: An attacker-centric gamified approach. *Technol. Innov. Manag. Rev.* **2015**, *5*. [[CrossRef](#)]
87. Bellekens, X.; Jayasekara, G.; Hindy, H.; Bures, M.; Brosset, D.; Tachtatzis, C.; Atkinson, R. From Cyber-Security Deception to Manipulation and Gratification Through Gamification. In *HCI for Cybersecurity, Privacy and Trust*; Moallem, A., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 99–114.
88. Sadeh-Konieczpol, N.; Wescoe, K.; Brubaker, J.; Hong, J. Mock Attack Cybersecurity Training System and Methods. US Patent US9558677, 31 January 2017.
89. Toth, P.; Klein, P. A role-based model for federal information technology/cyber security training. *NIST Spec. Publ.* **2013**, *800*, 1–152.
90. Glumich, S.M.; Kropa, B.A. Defex: Hands-On Cyber Defense Exercise for Undergraduate Students. Available online: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a560055.pdf> (accessed on 11 December 2020).
91. Conklin, A. The use of a collegiate cyber defense competition in information security education. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 22–23 September 2005; pp. 16–18.
92. Dodge, R.; Ragsdale, D.J. Organized cyber defense competitions. In Proceedings of the IEEE International Conference on Advanced Learning Technologies, Joensuu, Finland, 30 August–1 September 2004; pp. 768–770.
93. Augustine, T.; Dodge, R.C. Cyber Defense Exercise: Meeting Learning Objectives Thru Competition. 2006. Available online: <https://tinyurl.com/y254qj3> (accessed on 11 December 2020).
94. Mattson, J.A. Cyber defense exercise: A service provider model. In Proceedings of the Fifth World Conference on Information Security Education, West Point, NY, USA, 19–21 June 2007; pp. 81–86.
95. Patriciu, V.V.; Furtuna, A.C. Guide for Designing Cyber Security Exercises. Available online: <http://www.wsea.us/e-library/conferences/2009/tenerife/EACT-ISP/EACT-ISP-28.pdf> (accessed on 11 December 2020).
96. Braje, T.M. *Advanced Tools for Cyber Ranges*; Technical report; MIT Lincoln Laboratory: Lexington, KY, USA, 2016.
97. Talbot, J.; Pikula, P.; Sweetmore, C.; Rowe, S.; Hindy, H.; Tachtatzis, C.; Atkinson, R.; Bellekens, X. A Security Perspective on Unikernels. In Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 15–19 June 2020; pp. 1–7.
98. Pham, C.D. On Automatic Cyber Range Instantiation for Facilitating Security Training. Available online: <https://dSPACE.jaist.ac.jp/dSPACE/bitstream/10119/14161/3/paper.pdf> (accessed on 11 December 2020).

99. Eckroth, J.; Chen, K.; Gatewood, H.; Belna, B. Alpaca: Building Dynamic Cyber Ranges with Procedurally-Generated Vulnerability Lattices. In Proceedings of the 2019 ACM Southeast Conference, Kennesaw, GA, USA, 18–20 April 2019; pp. 78–85.
100. Fok, C.; Petz, A.; Stovall, D.; Paine, N.; Julien, C.; Vishwanath, S. Pharos: A Testbed for Mobile Cyber-Physical Systems. Available online: <https://www.cs.odu.edu/~nadeem/classes/cs795-CPS-S13/papers/eval-001.pdf> (accessed on 11 December 2020).
101. Deckard, G.M. Cybertropolis: Breaking the paradigm of cyber-ranges and testbeds. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018; pp. 1–4.
102. Tranoris, C.; Denazis, S.; Guardalben, L.; Pereira, J.; Sargento, S. Enabling Cyber-Physical Systems for 5G networking: A case study on the Automotive Vertical domain. In Proceedings of the 2018 IEEE/ACM 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Gothenburg, Sweden, 27 May–3 June 2018; pp. 37–40.
103. Urquhart, C.; Bellekens, X.; Tachtatzis, C.; Atkinson, R.; Hindy, H.; Seem, A. Cyber-security internals of a skoda octavia vRS: A hands on approach. *IEEE Access* **2019**, *7*, 146057–146069. [[CrossRef](#)]
104. Mitra, R.N.; Agrawal, D.P. 5G mobile technology: A survey. *ICT Express* **2015**, *1*, 132–137. [[CrossRef](#)]
105. West, D.M. How 5G technology enables the health internet of things. *Brook. Cent. Technol. Innov.* **2016**, *3*, 1–20.
106. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.J.A. The roadmap to 6G: AI empowered wireless networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [[CrossRef](#)]
107. Bhardwaj, A.; Krishna, C.R. A Container-Based Technique to Improve Virtual Machine Migration in Cloud Computing. *IETE J. Res.* **2019**, 1–16. [[CrossRef](#)]
108. Lovas, R.; Kardos, P.; Gyöngyösi, A.Z.; Bottyán, Z. Weather model fine-tuning with software container-based simulation platform. *IDŐJÁRÁS/Q. J. Hung. Meteorol. Serv.* **2019**, *123*, 165–181. [[CrossRef](#)]
109. Mucci, D.; Blumbergs, B. TED: A Container Based Tool to Perform Security Risk Assessment for ELF Binaries. Available online: <https://www.scitepress.org/Papers/2019/73716/73716.pdf> (accessed on 11 December 2020).
110. Kyriakou, A.; Sklavos, N. Container-based honeypot deployment for the analysis of malicious activity. In Proceedings of the 2018 Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 23–25 October 2018; pp. 1–4.
111. Delicato, F.C.; Al-Anbuky, A.; Kevin, I.; Wang, K. Smart Cyber-Physical Systems: Toward Pervasive Intelligence Systems. *Future Gener. Comput. Syst.* **2020**, *107*, 1134–1139. [[CrossRef](#)]
112. Kaloudi, N.; Li, J. The ai-based cyber threat landscape: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–34. [[CrossRef](#)]
113. Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitsoff, T.; Filar, B.; et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv* **2018**, arXiv:1802.07228.
114. Bécue, A.; Fourastier, Y.; Praça, I.; Savarit, A.; Baron, C.; Gradussofs, B.; Pouille, E.; Thomas, C. CyberFactory# 1—Securing the industry 4.0 with cyber-ranges and digital twins. In Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 13–15 June 2018; pp. 1–4.
115. Reys, N. Smart Cities and Cyber Threats, ControlRisks. Available online: <https://www.controlrisks.com/-/media/corporate/files/our-thinking/insights/smart-cities-and-cyber-threats/smart-cities-article.pdf> (accessed on 11 December 2020).
116. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [[CrossRef](#)]
117. Vitunskaitė, M.; He, Y.; Brandstetter, T.; Janicke, H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Comput. Secur.* **2019**, *83*, 313–331. [[CrossRef](#)]
118. Mylrea, M. Singapore’s Smart City: Securing It from Emerging Cyber Threats. Available online: <https://dr.ntu.edu.sg/handle/10356/80353> (accessed on 11 December 2020).

119. Srivastava, S.; Bisht, A.; Narayan, N. Safety and security in smart cities using artificial intelligence—A review. In Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, Noida, India, 12–13 January 2017; pp. 130–133.
120. AlDairi, A.; Lo'ai Tawalbeh. Cyber security attacks on smart cities and associated mobile technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. [[CrossRef](#)]
121. Cerrudo, C. Hacking Smart Cities. Available online: <https://docs.huihoo.com/rsaconference/usa-2015/hta-t10-hacking-smart-cities.pdf> (accessed on 11 December 2020).
122. Alibasic, A.; Al Junaibi, R.; Aung, Z.; Woon, W.L.; Omar, M.A. Cybersecurity for smart cities: A brief review. In Proceedings of the International Workshop on Data Analytics for Renewable Energy Integration, Riva del Garda, Italy, 23 September 2016; pp. 22–30.
123. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [[CrossRef](#)]
124. Wang, P.; Ali, A.; Kelly, W. Data security and threat modeling for smart city infrastructure. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–6.
125. Farahat, I.; Tolba, A.; Elhoseny, M.; Eladrosy, W. Data security and challenges in smart cities. In *Security in Smart Cities: Models, Applications, and Challenges*; Springer: Cham, Switzerland, 2019; pp. 117–142.
126. Vattapparamban, E.; Güvenç, İ.; Yurekli, A.İ.; Akkaya, K.; Uluagaç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 216–221.
127. Li, Z.; Shahidepour, M. Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. *Electr. J.* **2017**, *30*, 52–61. [[CrossRef](#)]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).