

网络靶场研究现状与展望

邹星¹, 胡宁¹, 顾钊铨^{1,2}, 贾焰¹

(1.鹏城实验室新型网络研究部, 广东 深圳 518055; 2.哈尔滨工业大学(深圳)计算机科学与技术学院, 广东 深圳 518055)

摘要: 当今社会各种网络安全事件不断发生, 网络安全研究受到世界各国高度重视。为了更好地支撑网络安全技术研究, 避免攻防演练和技术验证对真实的网络和生产环境造成不良影响, 网络靶场应运而生。作为一种特殊的测试平台, 网络靶场可提供逼真、可控、灵活的实验环境, 能够有效降低研究成本、缩短研究周期、规避研究风险。因此, 网络靶场是支持网络空间安全技术研究的重要基础设施和世界各国高度重视的科学实验平台。随着网络靶场基础支撑技术和计算模型的不演进, 网络靶场正面临新的问题与挑战。因此, 介绍网络靶场的发展历程、典型分类及技术架构; 分析国内外工业界和学术界的研究现状, 归纳各国典型靶场的建设情况, 梳理靶场关键技术的研究进展; 总结网络靶场面临的挑战问题, 并展望网络靶场的未来发展趋势, 这项工作对国内网络靶场技术研究和网络靶场项目建设具有参考价值。

关键词: 网络安全; 网络靶场; 仿真技术; 建设框架

中图分类号: TP393.08

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024063

Cyber ranges: survey and perspective

ZOU Xing¹, HU Ning¹, GU Zhaoquan^{1,2}, JIA Yan¹

1. New Network Research Department of Pengcheng Laboratory, Shenzhen 518055, China

2. College of Computer Science and Technology, Harbin Institute of Technology, Shenzhen 518055, China

Abstract: Various cyber attacks occurred frequently. Increasing attention has been being paid to cyber security by many countries. To support research on cybersecurity technologies and to avoid the potential effects of attack and defense exercises and technical verification on real networks and production environments, numerous cyber ranges emerged. As a special type of testbed, cyber ranges provide a real, controllable, and flexible experimental environment that effectively reduce research costs, shorten research cycles, and avoid research risks. Cyber ranges, being important scientific infrastructure and scientific experimental platforms, are highly valued by countries around the world. With the continuous evolution of basic support technologies and computational models, cyber ranges face new problems and challenges. This study introduced the development history, typical classification, and common architectures of cyber ranges. The current research status, core projects, and key technologies of industrial and academic cyber ranges in our country and foreign countries were analyzed and compared. Fi-

收稿日期: 2024-04-18; 修回日期: 2024-06-11

通信作者: 胡宁, hun@pcl.ac.cn

基金项目: 鹏城实验室重大攻关项目(PCL2023A07-4)

Foundation Item: The Major Key Project of PCL (PCL2023A07-4)

引用格式: 邹星, 胡宁, 顾钊铨, 等. 网络靶场研究现状与展望[J]. 网络与信息安全学报, 2024, 10(5): 1-22.

Citation Format: ZOU X, HU N, GU Z Q, et al. Cyber ranges: survey and perspective[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 1-22.

nally, the study summarized the challenges and difficulties faced by cyber range construction and proposed future research directions on cyber ranges. This work has reference value for conducting research and construction of cyber ranges.

Keywords: cyber security, cyber range, emulation technology, construction framework

0 引言

计算机网络和信息技术近年来飞速发展,极大地促进了经济发展和社会进步,同时也带来了新的安全风险和技术挑战。网络安全事关个人隐私、行业利益、国家安全,是关系国家主权、社会稳定等方面的重要问题,它随着全球信息化步伐加快显得愈发重要^[1]。针对日益复杂的网络安全问题,亟须支撑网络安全技术研究的基础设施,网络靶场(cyber range, CR)应运而生。与传统研究网络技术的测试平台(testbed, TB)相比,网络靶场专用于网络安全领域,除了具备真实网络环境的模拟和仿真能力,还可以提供网络攻防演练、攻击行为分析和研判等能力。网络靶场能够提供逼真、可控的试验环境,避免对真实网络空间造成破坏^[2]。经过二十多年的发展,网络靶场已成为世界各国进行网络安全科学研究、教育培训、测试验证、攻防演练等不可缺少的重要基础设施^[3]。各国基于网络靶场开展大量护网、众测、网络安全人才选拔活动,市场上出现了众多以网络靶场为主营业务的网络安全企业。网络靶场蕴含巨大社会和经济价值,是当前的热点方向。

随着时代变化,网络靶场出现了新的需求和技术,带来了新的挑战和趋势,亟须对国内外靶场研究现状重新梳理,为网络安全相关人员提供参考。本文调研国内外超30个靶场项目,总结网络靶场4个发展历程阶段、2个典型分类与3个常见架构,对比分析国内外工业界和学术界研究现状,总结各国的典型靶场项目,对比分析靶场经典综述工作,介绍靶场关键技术研究进展。阐述网络靶场当前面临的大规模网络仿真、攻击表达与检测、想定(Scenario)设计与开发等挑战,并展望未来发展趋势,以期为国内网络靶场研究提供技术参考与发展启示。

1 网络靶场背景

1.1 发展历程

2008年,美国国防部高级研究计划局(De-

fense Advanced Research Projects Agency, DARPA)首次提出了国家网络靶场(national cyber range, NCR)的概念和设计构想^[4]。DARPA认为网络靶场是推动网络安全研究和发展的重大科学装置,这便是网络靶场最初的定位。目前受到广泛引用的3种网络靶场定义分别来自美国、欧洲、中国。

1) 美国国家标准及技术协会(National Institute of Standards and Technology, NIST)^[5]面向网络安全教育、认证和培训领域提出:CR是对一个组织或机构的本地网络、系统、工具和应用程序的交互式模拟表示,即模拟环境。这些内容连接到互联网模拟仿真环境,为获取实际的网络技能提供安全、合法的训练环境,并为产品开发和态势测试提供了安全的环境。

2) 欧洲网络安全组织(European Cyber Security Organization, ECSO)^[6]认为:CR是用于开发、交付、使用的交互式模拟环境平台。模拟环境是对组织的信息通信技术、运行技术、移动和物理系统、应用和基础设施的表示,包括对攻击、用户活动、网络活动、依赖的第三方/公开服务的模拟。靶场包括仿真环境的核心技术以及必要的附加组件。

3) 中国网络安全领域的方滨兴院士研究团队^[3]认为:CR是针对网络攻防演练和网络新技术评测的重要基础设施,主要用户为政府和军队部门人员,通常用来提升网络和信息系统的稳定性、安全性和性能。结合方滨兴等2016年对网络靶场发展阶段的划分^[3]与当今靶场行业的发展现状,可以将全球网络靶场的发展历程大致划分为4个阶段,如表1所示。

1.2 典型分类

根据美国NIST在2023年发布的网络靶场指南中^[5]提出的基于实现技术的分类标准,可以把CR分为4类:模拟(Simulation)、仿真(Emulation)、叠加(Overlay)、混合(Hybrid)。早期的CR实现技术以模拟和仿真技术为主,随着云计

表1 网络靶场的发展历程
Table 1 Development history of cyber ranges

阶段	年代	技术路线	特点	主要产品
实物高逼真型靶标时期	21世纪初—2005年	针对敌方实体设备或系统,建立高逼真型靶标	①需要真实设备和网络 ②费钱费力 ③应用领域局限	蜜罐和木马系统等
小型虚拟化互联网靶场时期	2005年—2014年	利用仿真和虚拟化技术,构建小规模仿真网络环境	①无法达到预期仿真效果 ②无法用于实时演练 ③规模小,与实际系统差距大	小型靶场,如KYPO、CRATE等
大型虚实结合网络靶场时期	2014年—2022年	利用仿真、虚拟化、虚实结合技术,构建大规模仿真网络环境	①具备集成调度管控能力,可快速自动实现网络仿真环境 ②集成化、体系化、协同化发展 ③支持网络安全培训与测试	大型靶场,如NCRC、NATO CR等
跨域融合靶场时期	2022年至今	基于广域网环境,构建分布、自治的跨领域融合仿真网络环境	①支撑行业融合,实现不同行业靶场资源共享 ②各CR互联互通,丰富靶标和场景资源	联邦靶场,如ECHO、鹏城网络靶场等

算、虚拟化等技术的发展,目前大部分CR属于混合类。靶场实现技术对比如表2所示。

以应用领域为分类依据,可以把CR分为4类:科研类、教育类、企业类、军用类。部分功能全面的CR可能覆盖多个应用领域,如美国NCR既可用于军事演练,也可以用于科学研究,普通CR大多针对某个核心应用领域而研发。各CR应用领域的主要目标用户、特点和国内外典型靶场示例对比如表3所示。

1.3 靶场架构

1.3.1 NIST架构

NIST发布的网络靶场指南中^[5]提出针对网络安全教育培训领域的CR架构^[5],该架构以靶场学习管理系统为核心,涵盖网络安全培训和攻防竞赛的各个环节和功能模块。NIST网络靶场

架构如图1所示,包括5个部分。

1) 靶场学习管理系统: CR的核心功能,包括各种应用功能,提供基于靶场的学习过程管理能力。

2) 编排层: 负责实现底层基础设施虚拟化、目标基础设施网格化等功能,最常用的编排工具包括CloudShell、OpenStack等。

3) 底层基础架构层: 包括本地服务器、专用硬件、云服务器等软硬件资源组成的基础设施,能够存储CR的业务数据。目前CR的底层基础架构趋向使用软件定义网络技术。

4) 虚拟化层: 虚拟化技术能够减少CR的物理设备投入,从而降低成本。主要包括基于虚拟化管理程序和基于软件定义的基础结构。

5) 目标基础设施层: 模拟生成目标网络场

表2 靶场实现技术对比
Table 2 Cyber range implementation technology comparison

分类	技术特征	优点	缺点	示例
模拟	基于真实网络组件重新创造合成的网络环境,不需要物理网络设备,运行在虚拟实例之上。典型的模拟环境中,虚拟机(virtual machine, VM)复制信息技术基础设施中特定的服务器、网络和存储等。模拟效果好坏决定了环境的真实性,通常需要强大的编排层	成本低	真实性低	SIMTEX
仿真	在专用的网络基础设施上,把已经构建的网络/服务器/存储基础设施映射到物理基础设施,物理的基础设施成为网络靶场,仿真提供经由多个环境互联的闭环网络。通过流量生成来仿真网络协议、网络流量、攻击和底层互联网互联性	高保真性,比较全面地复现真实网络环境	成本高,需要专用物理设施	NCR
叠加	运行在真实的网络、服务器和存储设备之上,叠加类靶场通常基于覆盖网络	具有更高的保真性	成本高,可能对真实网络环境产生不良影响	GENI
混合	由模拟、仿真、叠加3种靶场的任意特性组成	具备更好的适配性	实现技术复杂	Virginia CR

表 3 靶场应用领域对比

Table 3 Cyber range application area comparison

分类	目标用户	特点	国内典型靶场	国外典型靶场
科研类	研究人员	提供安全、逼真、可控的研究环境,用于网络安全研究、新技术验证等	鹏城网络靶场、贵阳国家大数据安全靶场、各单位自建科研靶场等	Virginia CR、JOSE、SECUSIM、RINSE、OPNFT CR、CYROP、CyTrone、JOSE 等
教育类	学生或社会大众	提供网络安全教学环境、职业资格认证、网络安全能力培养、攻防演练和比赛等服务	黄鹤网络靶场、VulFocus、CTFHub、XSS-LABS、各网络安全竞赛平台等	Michigan CR、Warrior CR、VulHub、DVWA、WebGoat 等
企业类	企业公司	开发具备行业特色的网络靶场,提供漏洞挖掘、风险验证、攻击防御和数字取证等服务	赛宁网络靶场、合天网络靶场、软极网络靶场、奇安信网络靶场等	Cyberbit、CybExer、Cisco CR、Circadence、Simpace、Cyrin、AWS CR、hns-platform 等
军用类	政府军队部门	由各国的政府机构和军事部门资助建设,成本高、规模庞大、技术复杂、功能丰富,用于增强国家网络安全力量	总装某靶场、军队专用靶场等	NCR、CSR、JIOR、JCOR、PCTE、FCR、NATO CR、IAR、CSR、C4AD、DECRE 等

景的基础设施,如给学生提供网络安全教学实训的模拟环境。靶场学习管理系统利用脚本通过编排层创建目标基础设施,脚本一般包括各种网络、环境配置信息等。

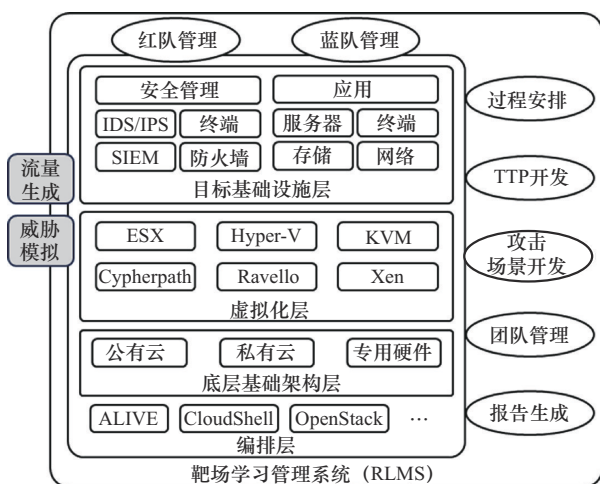


图 1 NIST 网络靶场架构

Figure 1 NIST cyber range architecture

1.3.2 ECSO 架构

ECSO 提出面向通用场景的 CR 架构^[6], 主要关注靶场能力和核心技术, 从用户到底层技术进行划分, 并列出基础的功能模块, 包括用户交互层、编排层、底层支撑技术层。Ukwandu 等^[7]扩充 ECSO 架构, 包括 4 部分 (前端技术层、靶场能力层、基础设施技术层、核心技术层), 增加前端技术细节和靶场能力模块, 并指定用户接口。ECSO 网络靶场架构如图 2 所示, 包括 3 个部分。

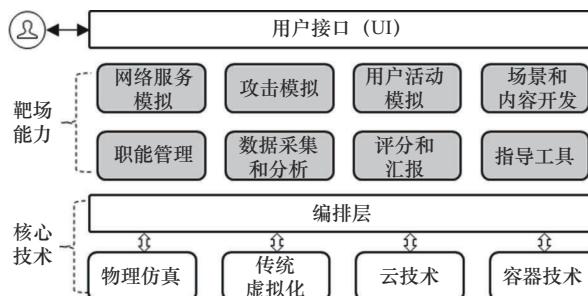


图 2 ECSO 网络靶场架构

Figure 2 ECSO cyber range architecture

1) 用户交互层: 采用 B/S 架构, 管理人员通过图形界面进行配置、监控和修改等操作。用户通过浏览器访问网络服务模拟、攻击模拟、用户活动模拟、场景和内容开发等靶场能力。

2) 编排层: 编排层通常对用户不可见, 是 CR 的重要组成部分, 能影响 CR 的可用性和成本, 负责对计算机系统和软件进行自动化配置、协调和管理, 创建自动化 workflow, 包括 VM 创建、修改和删除等; 虚拟基础设施和组件的配置、任务自动化等; 支持想定场景, 协调虚拟环境, 实现 CR 中不同组件的交互等。

3) 底层支撑技术层: 常见底层技术包括物理仿真、传统虚拟化、云技术、容器技术 (以 Docker 为代表) 等, 提供底层网络仿真功能。底层支撑技术层与编排层共同组成靶场的核心技术。

1.3.3 鹏城靶场架构

鹏城网络靶场是由大量软硬件设备组成的分布式仿真平台, 覆盖通信、电力、金融、汽车等

行业，能够仿真出一组目标网络、提供安全事件检测评估服务。其体系架构采取分层结构，各层协同工作，实现高效、灵活的目标场景仿真。用户通过靶场基础平台访问靶场环境，采用B/S架构。鹏城网络靶场架构如图3所示，主要包括资源层、网络层、仿真层和分析层4个层次。

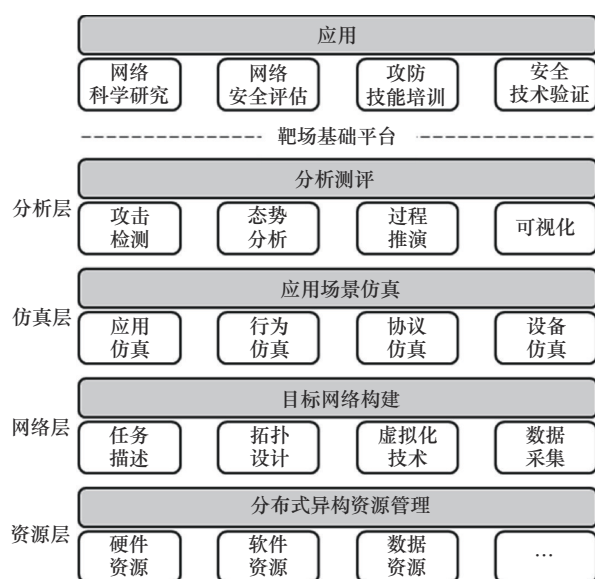


图3 鹏城网络靶场架构

Figure 3 Pengcheng cyber range architecture

1) 资源层：为靶场提供基础资源池，包括一组硬件、软件、网络、数据等资源，如高性能服务器、网络安全设备、攻防软件工具和系统镜像等，供上层使用和调度。底层的基础资源需要统一管理和配置，目前鹏城靶场基于云操作系统自主开发实现分布式异构资源管理。

2) 网络层：负责实现高效、灵活、逼真的目标网络环境构建，通过软件定义网络、虚实互联等技术快速生成目标网络拓扑，根据试验需求和任务描述等创建虚拟节点和仿真节点。基于图形界面完成可视化网络拓扑设计，为试验活动提供基础网络支撑，同时在网络层配置数据采集探针，收集网络数据，供后续数据分析和效果评估使用。

3) 仿真层：根据不同的应用场景提供应用、行为、协议和设备等仿真功能，基于真实网络流量数据和多种流量混合模型，实现高保真业务场景仿真，使试验活动的场景更加逼真。鹏城靶场目前可支持多种常见的网络协议

和应用仿真工具，已建立丰富的靶标库和场景库。

4) 分析层：提供基于靶场试验活动的分析功能，如攻击检测、态势分析、过程推演、训练效果评估、分析数据可视化呈现等。按照网络攻防的全生命周期，将数据分析分为4个阶段：采集、分类、分析、呈现。鹏城靶场通过在目标网络上部署大量检测设备和节点探针，支持靶向性、细粒度地收集网络流量数据和系统日志数据。可视化模块提供基于定量评估计算模型和方法的网络安全态势分析和评估。

1.3.4 对比分析

通过比较3个架构可以发现，现代化CR都将虚拟化技术作为基础支撑技术，在对底层物理资源进行虚拟化后，进一步通过资源编排技术构建具有不同业务能力的目标网络。不同CR架构的差异主要体现在应用层的设计。NIST面向教育培训，其应用层强调对固定应用场景的快速构建能力。ECSO架构关注CR基础能力的建设，对CR的应用模式缺乏讨论。鹏城网络靶场将CR的应用归结为4种典型方向，并在应用层针对不同应用方向做了功能性设计，从而提升CR作为网络安全研究基础设施的服务能力。

2 工业界研究现状

网络靶场研究大致可分为工业界（项目）领域和学术界（科研）领域，彼此之间紧密关联。工业界主要以项目工程为核心，项目规模较大，目标是建立可支撑各种现实试验活动的软硬件平台，可以投入现实场景使用，满足军队演练、网络安全培训等不同领域需求。学术界主要以技术为核心开展科学研究，优化实现技术、提升靶场运转效率等。基于大型工业项目的研究主要偏向总体架构设计和系统原型构建，基于小型科研项目的研究通常针对靶场关键实现技术进行设计和优化。

2.1 国内外靶场建设对比

本节对国内外工业界超30个典型项目进行分析，对比国内外靶场建设现状，总结典型网络靶场，为国内靶场项目建设提供参考。近年来，美国、欧洲等的网络安全演习场景具备全方位、多领域、全面覆盖等特点，网络安全演习规模再

创新高,网络靶场建设加速,攻防演练场景更加多样和完善^[8-9]。在CR项目建设方面,国外CR的研究建设开始较早,相关技术积累丰富,但大部分的CR非开源,少量科研类靶场开源,技术资料有限。

国内外网络靶场现状对比如表4所示,目前美国靶场建设处于领先地位,欧洲各国处于上游地位,国内处于发展与跟进阶段。相比中国、美国、欧洲,其他国家CR项目较少。

1) 加拿大: FIELD Effect是知名的私营商业公司。部分大学与美国公司合作建设CR,包括渥太华大学与IBM X-Force合作、多伦多都市大学与SANS公司合作建立Rogers Cybersecure Catalyst项目等。

2) 日本: 目前独立研发的CR较少,在TB领域起步早,2000年年初研制通用测试床StarBED,经过多年发展,如今第五代能仿真真实环境。2017年研制的CyTrone开源框架可支持基于CR的网安培训。与美国SANS、谷歌等合作推进CR建设,与欧盟合作建设FESTIVAL、FELIX等科研项目。

3) 韩国: 近年来与美国建立战略网络安全合作框架,参与美国主导的CR演习,但基本没有大型CR项目,主要依托美国支撑网安建设。

4) 以色列: CR商业水平高,著名公司包括Cyberbit、CyberGym等,主要提供基于CR的网安培训服务和产品,拥有众多网安领域的商业公司,如WaterFall、Cyber-Ark等。

各国典型网络靶场如表5所示。在全球范围内,美国和欧洲建设CR的数量处于领先地位

位^[10]。中国建设的靶场数量处于中等水平。近年来,中国网络安全领域市场活跃,CR数量增长迅猛。其他国家的CR建设数量较少,如加拿大、日本、韩国、俄罗斯等^[11]。大部分国家的靶场项目包括国家级靶场,这种类型的靶场一般由政府资助,主要用于加强国家网络安全建设,具有网络规模大、成本投入高、建设周期长等特点。

2.2 国内外典型靶场分析

2.2.1 美国

美国在CR建设方面拥有二十多年的技术积累,靶场建设处于全球领先地位,CR建设数量多且发展较为连续,每隔几年都会推出新的靶场项目或者产品。早年CR主要为军队和政府服务,用于军事演练和网络作战部队技能培训等。近年来军民融合趋势明显,出现了面向大众网安技能培训及各种商业领域的靶场。表6中列出近年来美国典型的网络靶场。

调研有如下发现。①在实现技术方面,CR实现技术从早期的模拟技术逐渐向虚实结合的混合类型转变。②在应用领域方面,美国CR早期主要为军队提供服务,大部分靶场项目与军事演练需求相关。③在架构方面,出于CR间协同共享资源等需求,靶场架构从早期的集中式靶场逐渐转向分布式靶场,不仅建立国内的互联靶场,也会与其他国家合作建设海外节点。④美国网络靶场技术把控严密,基本没有开源类的靶场项目。

2.2.2 欧洲

欧洲CR建设位于世界前列。欧洲CR类型

表4 国内外网络靶场现状对比

Table 4 Comparison of the current situation of domestic and foreign cyber ranges

现状	中国	美国	欧洲
发展现状	处于发展跟进阶段,CR数量比国外少,技术在学习发展中,与国外交流合作少	处于领先地位,建设CR数量多,技术先进,与盟友国合作紧密	处于上游地位,建设CR数量多,与美国等技术合作紧密
规模大小	大部分CR规模较小,知名国家级靶场为贵阳国家大数据安全CR和鹏城网络靶场,其他主要是教育类CR和公司研发的商业CR	CR规模覆盖广泛,有联邦、国家级、城市级CR,也有面向行业、教育的小型CR和商业CR	CR规模覆盖广泛,有联邦、国家级CR,也有面向不同行业的CR,与美国合作的CR等
应用领域	国防军事、攻防演练、网安竞赛、教育培训、人才认证、风险评估	国防军事、攻防演练、网安竞赛、教育培训、人才认证、风险评估、网络战部队训练、工业系统安全、游戏化培训	
产学研现状	具有国际影响力的CR较少。科研院所自主化开发较难,市场化较难,技术创新难。企业产品之间存在技术壁垒,产学研合作不足	大型CR通常与军工背景的企业合作,教育类CR与学校合作,产学研合作紧密,国家之间也有技术合作	

表 5 各国典型网络靶场
Table 5 Typical cyber ranges in various countries

国家	网络靶场	数量
中国	国家级：贵阳国家大数据安全靶场等 商用：360、绿盟科技、永信至诚、合天网安、赛宁网安、博智安全、奇安信等企业建设的靶场 科研：中国航天科工、鹏城实验室、中科院信工所、电子六所等单位建设的靶场	15+
美国	国家级：NCR、NCRC、JCOR、JIOR、PCTE、IAR、CSR、C4AD、DECRE、SIMTEX、CAAJED、StealthNet 等 商用：Cisco CR、Circadence、Simpac、Cyrin、U.S. Cyber Range、SANS、MCR、X-Force Command、AWS CR 等 科研：SECUSIM、RINSE、OPNFT CR、VCSTC、Emulab、DETER、Virginia CR、NetEngine 等	30+
欧洲各国	国家级：CRATE、SATURN、Federated Cyber Range (FCR) 等 商用：hns-platform、CybExer、Breakingpoint、Silensec 等 科研：KYPO、CyberMAR、Cyber-SHIP、AIT、FORESIGHT、SPIDER、CONCORDIA、ECHO、CyberSec4Europe、CD TEXP 等	20+
加拿大	商用：Field Effect 等 科研：uOttawa-IBM Cyber Range 等	2+
日本	国家级：StarBED、NII-SOCS 等 科研：CyTrone、JOSE、FESTIVAL、FELIX 等	7+
韩国	科研：Multi-Cyber Range 等	1+
以色列	商用：Cyberbit、CyberGym 等	2+
俄罗斯	国家级：The National Cyber Range 等	1+

表 6 美国典型的网络靶场
Table 6 Typical cyber ranges is the United States

名称	启动年	类型	架构	核心定位	应用场景	技术特征
JCOR	2003	模拟	集中式	美军多兵军种模拟器建模的专网环境的测试环境联合体	军事作战培训	虚实结合，模拟器，分布式部署与控制
JIOR	2003	仿真	集中式	美军多兵军种网络测试环境联合体	军事演练培训	虚拟化环境，建模，计算机仿真，模块化开发与集成
TENA	2005	仿真	分布式	军事领域联邦靶场资源互操作和可重构技术	连接分布式资源，建设联合试验能力	虚实结合，资源共享与重用
NCR	2008	仿真	集中式	国家级的军民融合 CR	网络武器测评，人才培养，验证评估 TTP	虚实结合，安全要素全仿真
CSR	2010	混合	集中式	模拟美军国防相关企业网络环境	军事演练培训，提升防御能力，验证评估 TTP	虚拟化，SDN，B/S 架构
Michigan CR	2012	混合	集中式	公开网络安全类培训 CR	网络安全教育，人才培训认证，攻防演练	B/S 架构
NCRC	2016	混合	分布式	国家级分布式 NCR	提升 NCR 容量和可扩展性	分布式网络集成，资源互联与共享
PCTE	2016	混合	集中式	网络任务部队训练的资源整合大型 CR	军事作战培训，场景事件管理，任务演练，TTP	虚实结合，云计算，人工智能，大数据，数字孪生
ACRE	2017	混合	集中式	可定制的商业网络靶场	多种场景，包括交通系统、工业控制系统、医疗系统等	精确模拟环境，事件同步，安全本地私有云
Space Range	2020	混合	集中式	虚拟可控的卫星指挥与控制仿真环境	保护美国政府和军方部门以及太空航天领域企业建设的太空系统网络安全	虚拟硬件复现太空操环境，软件定义基础设施 SDI，卫星互联网流量仿真
NAWCAD CR	2023	混合	分布式	美国国防部海军航空站关键测试资产	针对飞机及其子系统和支撑技术提供网络安全测试和培训计划	通用核心架构和工具集，支持分布式演习

大致可分为3类。①与美国合作：由美国支持或者参与建设，如英国联邦靶场、北约靶场（NATO CR）等；②欧洲国家独立建设：由政府军方资助建设，如瑞典CRATE、英国Cyber-SHIP等；③欧盟联合建设：由欧盟多国合作建设，旨在保护各成员国网络安全，如欧盟地平线2020计划（H2020）中的CONCORDIA、ECHO、Sparta和CyberSec4Europe项目。

表7中列出了欧洲典型的网络靶场，可以看出：①近年来欧洲建设联邦类型的靶场较多，且积极开展合作，重视构建网络安全技术共享社区；②欧洲靶场建设重点关注保护关键基础设施和保障公共网络安全；③欧洲建设的CR通常会有对应的公开网站，提供各种CR技术资料，公布靶场项目的目标、进度等信息，根据保密等级公开可共享的技术文件。

2.2.3 中国

国内典型的网络靶场如表8所示。国内CR大部分由科研机构、高等院校、网安企业等开发

建设。调研发现：①国内大型CR较少，大型CR代表有贵阳国家大数据安全靶场等；②大部分CR是面向不同领域的集中式单点靶场，仿真能力有限，仿真场景单一，无法满足分布式攻防演练需求，目前国内正在建设联邦靶场，突破靶场关键技术；③国内商业CR主要提供攻防演练、网络安全培训、比赛平台服务，应用场景有限。

3 学术界研究现状

3.1 国内外研究现状对比

根据国内外网络靶场发表论文规律，可将CR学术研究分为3个阶段：2000年至2008年的缓慢探索阶段，2009年至2013年的稳定发展阶段，2014年至今的高速发展阶段^[12]。

调研发现：①研究热度方面，近期国外相比国内更为活跃，研究工作数量更多；②热点方向方面，近期国外研究热点为基于CR的教育培训和想定管理，学术工作数量多且更新较快。目前国内靶场研究工作更多是围绕CR模拟仿真、流

表7 欧洲典型的网络靶场

Table 7 Typical cyber ranges in European

名称	启动年	类型	架构	核心定位	应用场景	技术特征
CRATE	2008	仿真	集中式	瑞典国防局建设的竞赛演练靶场环境	实战演练和武器装备测试	虚实结合,虚拟化,云计算平台
KYPO	2013	模拟	集中式	开源的竞赛演练平台	人员培训,攻防演练	开源,使用容器,基础设施即代码,微服务,云计算
hns-platform	2014	混合	集中式	提升网安技能的解决方案	教育培训,竞赛演练,测试验证	虚拟化,虚实互联
CD TEXP	2014	混合	分布式	各国靶场实时互联	网安防御,远程培训,跨国演习	资源协调,联邦共享
CybExer	2016	混合	集中式	提供网安培训解决方案	培训,竞赛,安全测试和评估	云计算,虚拟化,导调
AIT	2017	混合	集中式	工控领域平台	网安教育,技术研究和测试	虚拟化,云计算平台
Cyber-MAR	2019	模拟	集中式	海事网安决策平台	人员培训,网安攻防,风险评估和应急响应	LMS,风险框架,编排器
FORESIGHT	2019	混合	分布式	多行业协同联邦靶场	人员培训,联邦协同训练	身份服务,通信服务,协作服务
SPIDER	2019	混合	集中式	针对5G的CRaaS平台	人员培训,知识共享合作,攻防测试	5G环境,组件化,虚拟化
Cyber-SHIP	2019	混合	集中式	海事领域测试验证平台	软硬件测试验证,弹性测试	虚实互联,资源整合
CONCORDIA	2019	仿真	分布式	统一接入平台	网安培训,共享场景	网络架构仿真,自动化攻击
ECHO	2019	混合	分布式	多行业融合解决方案	建立面向基础设施的网安生态	管理模型,多方评估,协作共享
CyberSec4Europe	2019	混合	分布式	轻量级试点整合靶场	行业领域融合,开放实验室环境	虚拟化,容器,互操作性标准

表 8 国内典型的网络靶场
Table 8 Typical cyber ranges in China

名称	建设机构	规模大小	研究内容
贵阳国家大数据安全靶场	贵州数安汇大数据产业投资有限公司	大型	大型靶场,探索建设全国首个国家大数据安全靶场,主要用于攻防演练和国家安全防护,提供人才认证、攻防演练、网安比赛等服务
鹏城网络靶场	鹏城实验室	大型	大型靶场,可实现超大规模的网络仿真验证,突破百万节点规模的目标网络快速部署、面向业务场景的目标网络流量逼真模拟等关键技术
某军用靶场	中国人民解放军国防科技大学	中等	基于网络虚拟化技术构建的靶场,实现目标网络灵活构建,能够完成高性能虚拟链路仿真
网络攻防演练系统	中国电子科技集团公司电子科学研究院	中等	基于云平台开发建设网络攻防作战模拟系统,针对网络攻击等电子作战手段进行攻防试验,以加强网络信息系统安全
奇安信护网演练平台	奇安信科技集团股份有限公司	中等	针对护网行动构建的网络仿真验证平台,支撑攻防演练,重点研究网络攻击行为的实时检测等技术
黄鹤网络靶场	华中科技大学	小型	针对网安人才培养和网安竞赛等需求构建的靶场,重点研究网络攻防资源库、网安课件以及攻防演练平台建设

量生成等关键技术;③由于CR的敏感性,国内外学术研究存在一定技术壁垒。

3.2 综述领域研究

表 9 列出近十年来网络靶场领域的经典综述工作对比。在网络靶场领域总体综述方面,早期的靶场综述反映了当时环境下作者对靶场的认知和思考及国内外的靶场研究现状。本文工作结合最新的靶场技术需求与挑战,梳理近年来靶场项

目与学术工作,期望带来新的思考与启示。

笔者调研发现:①随着时代变化和技术演变,综述的重点和内容发生了变化,早期以实现技术为主,靶场项目较少,目前重点关注CR的使用;②近年靶场综述体现了新的技术趋势和新需求,如近年来靶场逐步使用SDN^[13]、容器技术、AI技术等,在国外综述中,任务想定等内容越来越受到关注,国内综述较少涉及该领域。

表 9 综述工作对比
Table 9 Comparison of survey work

文献	年份	引用次数	关注领域	国内外研究对比	关键技术	任务想定	关键问题和挑战	未来方向
李秋香等 ^[10]	2014	7	各国项目	⊙	⊙	○	○	⊙
方滨兴等 ^[3]	2016	23	各国项目和关键技术	●	●	○	●	●
王佰玲等 ^[14]	2021	1	工控靶场关键技术	●	●	○	●	●
李馥娟等 ^[2]	2022	0	各国项目和关键技术	●	●	○	○	●
张淼等 ^[15]	2023	0	建模与仿真服务化	●	●	○	○	●
邱志明等 ^[16]	2023	2	训练系统仿真	●	●	○	○	●
Davis ^[17]	2013	105	靶场和试验平台	●	●	○	⊙	●
Holm ^[18]	2015	138	工业控制试验平台	●	●	○	●	●
Vykopal ^[19]	2017	115	靶场和试验平台	●	●	○	●	●
Priyadarshini ^[20]	2018	44	靶场特征和架构	●	⊙	⊙	⊙	●
Yamin ^[21]	2020	248	靶场和试验平台	●	⊙	●	●	●
Ukwandu ^[7]	2020	92	靶场和试验平台	●	⊙	●	●	●
Chouliaras ^[22]	2021	75	教育培训领域的靶场	●	⊙	⊙	●	●
Glas ^[23]	2023	6	教育培训靶场	●	○	○	●	●
Vyron ^[24]	2023	15	无线安全测试床	●	⊙	○	●	●

注:●代表包含内容,○代表不包含,⊙代表部分包含,引用统计日期2024年6月5日

本文调研目前国内外最新 CR 项目和技术,且首次梳理国内外想定工作,涵盖内容全面,期望为 CR 领域研究提供启发与参考。

国内 CR 综述工作对国内外的项目调研数量较少,且均没有涉及任务想定方面的调研,覆盖内容不够与时俱进。这些靶场综述工作反映了国内靶场建设的定位演变趋势,从早期简单的网络安全试验平台逐渐过渡到功能复杂的大型网络安全基础设施。

2014 年,李秋香等^[10]介绍 CR 定义,认为网络靶场是网络安全试验平台,并总结网络靶场的 4 点特征(仿真性、广泛性、自动化、综合性);然后重点分析美国 NCR 的相关信息,简述英国、澳大利亚、俄罗斯等国的靶场现状,为我国建设靶场提出建议。该综述对 NCR 分析较为全面,但时效性较低,无法反映近年 CR 的发展。

2016 年,方滨兴等^[3]对 CR 关键技术进行调研,总结靶场定义、主要功能、演变阶段等,并分析美国、英国、日本、加拿大等国的靶场现状,从大规模网络仿真、网络服务和用户模拟、数据采集和评估、平台安全及管理这 4 个方面总结关键技术进展、提出挑战和未来发展趋势。该综述对于 CR 演变阶段的划分具有参考性,但时效性较低,缺少近年 CR 的进展。

2021 年,王佰玲等^[14]面向工业控制系统调研工控靶场和工控蜜网的关键技术,将工控安全仿真平台分为 3 类(工控测试床、工控 CR、工控蜜网),从虚拟化技术、靶场构建技术、蜜网诱捕技术、采集评估技术这 4 个方面对国内外研究现状进行总结和对比,并且分析面临的挑战和展望未来发展方向。该综述主要面向工控领域,具有领域局限性。

2022 年,李馥娟等^[2]调研 CR 关键技术领域,总结靶场的定义、基本功能,并分析美国 JIOR、JCOR、NCR、PCTE 等靶场,指出国内 CR 规模较小、应用较为单一;接着分析总结大规模网络仿真、网络流量模拟、用户行为模拟这 3 个方面的关键技术,认为目前难点是大规模网络流量模拟,未来发展方向包括:全频谱 CR、下一代 CR、多技术协同、工业互联网 CR。该综述涵盖内容全面,但是缺少想定设计领域的研究工作。

2023 年,张淼等^[15]介绍建模与仿真服务的概念、特征、发展演化等,分析基于云的建模与仿真服务化构建原则、基本架构、应用模式等,总结关键支撑技术。该工作可参考建模与仿真服务,但应用到 CR 存在难度。

2023 年,邱志明等^[16]针对体系对抗下的实战化模拟训练,总结联合训练领域的仿真体系架构、仿真建模、蓝军模拟、信息体系仿真等技术。该工作对于 CR 模拟仿真技术有参考价值,但主要针对训练系统。

国外的 CR 总体综述工作较多,通常不区分 CR 与 TB。靶场研究热度相比国内更高,大部分国外综述没有涉及国内靶场信息。

2013 年,Davis 等^[17]详细调研现有军事、学术、商业 CR,发现 CR 的主要角色是测试、训练、研究和开发,其中训练是最常见的用途。根据 CR 实现技术,将 CR 分为模拟类、仿真类和叠加类。模拟技术高效、可扩展但是不够逼真。仿真技术能提供高逼真和可重复性,但是昂贵且可扩展性不足。在当时的环境下,作者认为混合类 CR 的技术会越来越流行。该综述的技术分类启发了后续 NIST 等工作的 CR 分类,但是时效性较差。

2015 年,Holm 等^[18]调研工业控制系统测试床,调研 30 多个不同的 TB,大部分的设计目的是漏洞分析、教育和测试。调研不同领域(控制中心、通信网络、现场设备、物理流程等)的实现技术,以及虚拟化技术的实现方法,作者认为现场设备是最难虚拟化的部分,因为缺乏虚拟化平台的支持。该综述针对工控领域,同样具有领域局限性和较差时效性。

2017 年,Vykopal 等^[19]调研 2013 年至 2017 年的 CR 和 TB,分析 30 个 CR,大部分的用途为训练和教育,认为基于云计算、虚拟化、容器等技术的 CR 在快速发展。基于 KYPO CR 讨论 CR 的高层需求和架构,包括网络拓扑和软件系统的灵活性、可扩展性、隔离性和互操作性的平衡、高效的成本、内置的监控系统、访问便捷等。该工作针对国外 CR,缺少全面的对比分析。

2018 年,Priyadarshini 等^[20]调研 CR 的特征和架构,对欧美等国的多个 CR 进行分析,从基

基础设施组织架构、是否使用云、是否使用团队角色、是否部署VM这4个角度对靶场进行分类；调研美国多个州的CR，提出高校中理想的CR架构，并对不同需求进行紧急程度划分，对于校园靶场建设具有参考意义。该工作可参考欧美CR项目现状，但是同样缺少想定领域的研究。

2020年，Yamin等^[21]调研CR和TB的想定、功能、工具和架构，根据设定的分类依据，提出统一CR架构，发现近年来研究想定的科研文献最多，想定主要目的在于测试和教育，想定的类型动态偏多。未来的研究方向包括提升效率、可扩展性、联邦CR、用户行为模拟等。该综述内容丰富，但聚焦于国外CR工具，未涉及国内CR。

2020年，Ukwandu等^[7]调研目前和未来的CR和TB，对学术界和工业界对比分析，介绍了CR的架构设计、实现步骤；总结CR和TB的区别，发现CR应用领域从网络安全逐步转向培训、教育和研究，目前公开和联邦的CR类型最多，使用的技术中模拟类方法最多，其次是仿真与叠加。未来研究方向包括实时自动配置系统、增强现实技术辅助培训、5G/6G应用场景等。该综述内容详实，但缺少想定工作对比。

2021年，Chouliaras等^[22]利用问卷调研教育、培训和研究的CR和TB，对比CR的目标、环境类型、特征、工具。发现目前教育领域的CR提供安全课程包括网络安全、Web安全、数

字取证、软件安全等。CR主要采用基于模拟的技术，这一点与Ukwandu等^[7]的结论一致。最常用的工具包括OpenStack、VirtualBox等，常用的脚本是JSON和YAML。未来研究趋势包括支持新技术、提升CR使用便捷度、高效部署等。该综述基于问卷的形式较为新颖，但主要聚焦于教育领域，较为局限。

2023年，Glas等^[23]调研靶场演习CRX现状，提出分类框架TARGET，全面结构化评估各种CRX，结合问卷区分CRX优劣。他们发现目前CRX需要加强对参训人员的监督，以及提升SIEM系统水平。该综述有助于提升国内演习水平，但对CR建设帮助不大。

2023年，Vyron等^[24]调研无线安全领域的测试床，针对多领域，发现无线技术应用过程中存在安全问题，需要平衡测试床的功能性与安全性。该综述面向无线安全领域，具有领域局限性。

3.3 关键技术研究

CR通常基于靶场基础设施建设，涵盖多种关键技术，基于各种核心功能组成靶场建设框架。关键技术对比分析如表10所示。

3.3.1 模拟技术

模拟是指建模系统或者过程，使用软件去模拟某个系统或过程的功能，不一定实现内部细节，只保证在同样的输入下，系统或过程的输出

表10 关键技术对比分析
Table 10 Comparison of key techniques

关键技术	应用场景	分类	研究现状	常用工具
模拟	支撑教育、网络研究、网安实验、虚拟实验室等	网络服务模拟	技术发展成熟，常见协议如TCP、UDP、HTTP等多种工具可供选择	QualNet、Simulink、NS2、NS3等
		用户行为模拟	仍在发展中，目前大部分CR缺乏对用户行为的动态模拟 ^[25]	AutoIT、GHOSTS、Netkit、Kathara、Bespoke等
		攻击行为模拟	技术成熟，适合安全测试场景	Nmap、Nessus、Metasploit、THC-Hydra、tfn2k、LOIC等
仿真	用于测试床，评估端到端系统或协议的性能	网络拓扑仿真	技术较为成熟，现有软件工具需适配改造才能应用到CR	QualNet、Simulink、Cisco Packet Tracer、GNS3、Emulab、NetEM等
		网络流量仿真	研究热点，传统方法如解析建模合成、真实流量回放等难以适应CR复杂网络场景和环境 ^[25]	OpenFlow、5Greplay、Emulab、Flashback、DNP3等
虚拟化	适用于大部分CR，可减少CR成本，提高资源利用率和灵活性等	传统虚拟化技术	技术发展成熟，已有多种产品	VirtualBox、VMware、KVM、XEN、QEMU、Docker等
		云虚拟化技术	技术发展成熟，已有多种产品	OpenStack、OpenNebula、AWS、Google Cloud、CloudStack等

和所模拟系统的输出一致，可以看作原系统或过程的一个更快速的版本。基于模拟器能开发许多辅助训练系统^[26]，基于已有知识完成较为准确的预测，典型的模拟器包括飞行器模拟器、天气预报等。CR 中模拟技术主要包括 3 类：网络服务模拟、用户行为模拟、攻击行为模拟。

1) 网络服务模拟：描述与特定场景相关的服务，如模拟社交网络、路由协议、服务提供商、域名解析和公钥基础设施等服务。网络模拟器会使用离散事件模型，允许离散的步骤，使用事件在模拟实体间通信，从而产生状态迁移，即基于事件触发状态变化从而产生输出结果^[27]。网络服务模拟能提供典型社交媒体应用和其他网络服务，增加 CR 场景的真实性。由于某些网络服务的复杂性，部分场景中不会模拟网络服务^[6]。如表 11 所示，根据应用领域划分，常见的网络模拟器可分为：通用实验类、移动网络类、教育类^[28]。

2) 用户行为模拟：模拟普通诚实用户行为，同样可以增加 CR 场景真实性。UAS 包括模拟环境的真实用户、虚拟客户端、虚拟用户、手机等，可以模拟用户与目标环境的交互，如用户浏览网页、查看邮件、观看视频、下载文件等行为。实现用户行为模拟主要基于建模、机器学习等技术^[29]。

3) 攻击行为模拟：包括模拟 CR 内、外的攻击。通常目标是半自动测试系统安全态势。传统的漏洞扫描技术主要寻找目标系统、网络和程序的漏洞缺陷^[30]，而攻击模拟工具则可以模拟安全杀伤链的不同阶段。攻击模拟能提供多种预定义的攻击选项，以及导入、创建自定义攻击^[31]。在隔离的 CR 环境中，创建试验想定时可定义攻击行为。一些学者设计了 CR 中攻击行为模拟工具，但应用领域较为局限。例如，Pan 等^[32]提出

自动渗透测试攻击工具 Scorpio，Jiang 等^[33]提出对自动网络攻击工具进行安全测试和部署的 CR 环境 Pandora，Antonopoulos 等^[34]提出支持海上网络安全人员决策的攻击预测引擎 ATTSE。

3.3.2 仿真技术

仿真是对整个系统或过程的状态、行为、结果和系统实现进行复现，通常利用软硬件共同仿真目标系统的各个部件，不一定能够准确反映目标的内部状态，但能真实地模拟系统的运行机制。仿真系统可以看作原始系统的对等版本，主要目的是分析整个系统的内部结构、任务流程、输出结果等。仿真器能辅助测试系统，典型的仿真器包括安卓仿真器、单片机仿真器等。网络化仿真技术一般基于现代网络技术，完成系统建模、试验运行、分析评估等活动。网络化仿真可以集成各类资源，提供协作工作环境和各种仿真工具，有利于提升复杂性问题的研究分析能力^[35]。针对大规模、高逼真网络的仿真需求，目前主流仿真技术基于云平台 and 虚拟化技术。CR 中网络仿真主要包括：网络拓扑仿真和网络流量仿真。

1) 网络拓扑仿真：网络拓扑环境是 CR 试验中重要的组成部分，在想定准备过程中需要根据网络拓扑设计构建虚拟网络环境。近期的工作如下。2017 年，Pham 等^[36]设计和开发 CyRIS 系统，能在 CR 内创建任意的网络拓扑、配置网络服务、配置转发规则，实现复杂网络拓扑仿真。2018 年，Schoonover 等^[37]提出精细控制、高保真的计算机网络仿真框架 Galaxy，自动化设计软件代理，支持快速、并行的实验。2019 年，Chen 等^[38]提出基于全虚拟化、轻量级虚拟化、网络仿真和物理设备四尺度集成的多尺度网络仿真技术，具有连通性、透明性、可扩展性、实用性，能够支持大规模网络实验。2019 年，刘渊

表 11 网络模拟器分类

Table 11 Classification of network simulators

分类	特点	示例
通用实验类	用于研究网络协议建模、网络路由、网络性能等	OMNeT++、ns-3、ns-2、OPNET 等
移动网络类	用于蜂窝网(3G、4G、5G)和无线网(Wi-Fi、蓝牙、Zigbee)，可快速复现复杂网络拓扑，节约新技术的测试评估、开发部署时间	GloMoSim、QualNet、COOJA 等
教育类	用于实验教学，具备高可用性、用户友好界面、可定制化等特点	Cisco Packet Tracer、GNS-3 等

等^[39]面向多尺度融合网络仿真提出拓扑映射方法，结合 KVM、Docker 等虚拟化技术，基于 OpenStack 云平台，利用多级图快速划分、映射并部署大规模网络虚拟拓扑。2023 年，王晓锋等^[40]针对基于卫星通信的互联网，结合其业务分布不均、动态性、拓扑结构复杂等特点，设计基于 OpenStack 云平台和容器技术的动态仿真体系架构，提出卫星链路分布式仿真算法，实现链路性能的快速同步，完成卫星网络拓扑的仿真和实时重构。

2) 网络流量仿真：用于验证新算法、协议和网络功能的正确性及其影响^[41]。流量生成工具只能重放捕获的网络跟踪，或者生成简单的数据包流，而未考虑 CR 真实用户行为^[42]。网络流量生成是 CR 中重要的一项功能，可看作网络服务模拟中的一部分。2019 年，Javali 等^[42]提出基于狄利克雷分布和混合分布网络流量生成器，结合马尔可夫模型，并使用大型会话数据集评估模型，该流量生成器支持交互式界面和多种操作系统。2020 年，李松等^[43]针对网络流量预测研究，结合高斯过程混合模型分析网络流量数据，进行数据归一化、相空间重构、输入混合模型等处理，并通过实验证明该方法可提升网络流量的预测准确率。2021 年，Lee 等^[44]提出非周期性背景流量仿真的方法，使用随机数和随机变换来消除背景流量的重复周期，使用随机数和随机排列来连接流量数据，不需要额外硬件，能使背景流量与恶意流量不易区分，更好地辅助攻防训练。2023 年，Du 等^[45]提出背景网络流量生成模型，基于动态词嵌入技术设计智能特征提取方法，将流量

特征元组数据转换为静态的字向量，基于对比学习模型，通过学习小样本的特征分布，生成高质量和大量的背景网络流量。2023 年，Huang 等^[46]提出网络仿真分布式流量回放框架，用于云平台上大规模、高保真的网络流量仿真，设计绕过内核的快速流量重放策略，缓解内核协议栈的高开销问题，提高单节点的流量重放性能。

3.3.3 虚拟化技术

虚拟化技术是靶场关键技术中唯一的、能允许创建经济高效模拟结果的技术^[47]。目前虚拟化技术较为成熟，大部分 CR 的试验环境可通过虚拟化技术实现，然而有些组件难以模拟，仍需要物理设备。在 CR 领域使用的虚拟化技术主要包括传统虚拟化和云虚拟化^[6]。①传统虚拟化技术：CR 对整个基础设施的底层物理资源进行抽象，虚拟机管理器（Hypervisor）可充分利用资源，降低成本。②云虚拟化技术：CR 更加灵活，但丧失部分数据控制权，可能存在隐私风险。典型虚拟化和云服务产品如表 12 所示。

(1) 传统虚拟化

在云计算技术发展之前建成的 CR 大多基于传统虚拟化技术，稳定性较好。传统虚拟化技术最常见的用途是建设数据中心，包括大量服务器，能实现高效管理，但缺乏动态编排能力。基于传统虚拟化的网络仿真器包括 CORE、Cisco CML、IMUNES、SEED Labs 等。传统虚拟化包括基于 Hypervisor 和基于容器。

1) 基于 Hypervisor：VM 之间通过虚拟机管理器进行隔离和物理资源访问控制。Hypervisor

表 12 典型虚拟化和云服务产品

Table 12 Typical virtualization and cloud products

分类		示例
传统虚拟化	Type 1	XenServer、KVM、Hyper-V 等
	Type2	VMware Workstation、QEMU、VirtualBox 等
基于容器		Docker、Containerd、runC 等
云虚拟化	公有云	iCloud、Google Cloud、AWS 等
	私有云	Azure 私有云、EasyStack 等
	混合云	根据需求结合 VPN 技术等搭建

又可分为两类。Type 1 虚拟化：裸机直接取代 OS，Hypervisor 充当计算机硬件和 VM 之间的中介，负责分配和使用各种硬件资源，常用于虚拟服务器场景，用于建设数据中心。Type 2 虚拟化：虚拟机管理器作为 OS 上的应用程序，常用于终端设备场景。

2) 基于容器：容器共享 OS 内核，通过绑定应用代码、配置、库和依赖，提升应用的可移植性，目前以 Docker 技术为代表。常见的基于容器的网络仿真器包括 Mininet、NEMO、OAI、srsRAN、openLEON 等。容器技术具有应用程序级别的虚拟化能力。在 CR 中，使用容器技术可以预配置复杂网络和通信，提供编排能力，使系统高效。但是，容器不能模拟真实系统，只是针对应用环境的模拟，模拟能力有限，因此局限于教学培训领域。

(2) 云虚拟化

CR 通常会使用云服务，主要包括以下 3 类：公有云、私有云和混合云。①公有云：支付即可得，但开发新功能面临云服务提供商的技术限制。②私有云：适合需要保密和隐私的 CR，适合军队、政府等。③混合云：可灵活选择公有云和私有云，但需要划分数据权限、考虑每种云上存放的业务和数据、环境配置等。CR 中最常用的云平台包括 OpenStack、Google Cloud 等。

3.4 靶场建设框架

CR 建设不仅需要模拟、仿真、虚拟化等技术，也需要上层核心功能支撑。CR 建设框架主

要包括 3 部分，想定设计与开发是近年来国外 CR 中的热点研究方向之一，数据采集与评估支撑 CR 试验任务和比赛效果评定，管理与监控保障 CR 高效稳定运转。核心功能对比分析如表 13 所示。

3.4.1 想定设计与开发

早期在 CR 中举办网络安全培训等活动是人工配置完成的，非常耗时且容易出错，需要大量的技能要求，于是出现了 CR 想定的概念。CR 想定是指计划、设计和开展一系列基于 CR 的试验活动，相当于整个试验活动的剧本，规划不同难度的攻防场景，举办攻防演练竞赛、CTF 大赛、安全测评等试验活动。想定设计通常需要：描述试验活动基本信息、定义目标网络拓扑、配置攻防工具和底层基础设施等。攻防演习的质量取决于想定设计，自定义开发想定的功能可大幅提高 CR 的实用性和附加价值。

CR 试验活动中的各类用户通常用颜色区分，不同的项目对团队角色的定义不同^[21-22]。各方团队角色各有分工、相互配合，共同完成基于 CR 的试验活动。靶场中的五方角色如表 14 所示。

想定生命周期是指一次试验活动从规划到结束的流程。如图 4 所示，结合 Yamin 等^[21]提出的 6 个想定生命周期阶段与常见的五方角色，阐述各方参与想定生命周期的过程，为 CR 的想定设计和试验流程控制提供参考。

表 13 核心功能对比分析
Table 13 Comparison of core functions

核心功能	应用场景	分类	研究现状	常用工具
想定设计与开发	适合夺旗赛(capture the flag, CTF)、网络安全防御演习(cyber defense exercises, CDX)等比赛活动的设计与规划	想定设计与开发	目前国内基本没有 CR 想定领域的研究工作，国外研究大部分基于脚本语言设计	XML、JSON、YAML、自定义脚本语言等
数据采集与评估	适合需要数据分析的 CR 场景	数据采集	发展成熟，可用开源软件或定制采集探针等	Wireshark、Tcpdump、IPRoyal、Packetbeat 等
		分析评估	研究热点，目前大部分 CR 难以做到实时、准确、高效和全面评估	ScorBot、Jeopardy board、Flags、ICTF Board 等
靶场管理与监控	大部分 CR 需要管理与监控功能，属于基础功能	管理	国外大部分 CR 基于基础设施即代码(IaC)工具，国内大部分 CR 基于云平台定制管理功能	Terraform、Ansible、Chef、Puppet、OpenStack、Xentop 等
		监控	目前大部分 CR 使用运维管理工具	Zabbix、Prometheus、Nagios、OSSEC、Snort、Suricata 等

表 14 靶场中的五方角色
Table 14 Five roles in cyber ranges

角色	定位	主要责任
黄方	导调管理方	负责想定规划和试验控制。收集需求、制定计划,控制管理试验过程,复盘试验过程等
白方	技术保障组	负责环境搭建和技术维护。职责包括虚拟网络生成、网络拓扑配置、资源管理等
绿方	评估分析方	负责收集和分析试验运行数据。职责包括收集数据、评估攻防效果、分析试验数据等
红方	攻击方	在试验前制定攻击计划,进行攻击技术研制与部署。在试验过程中,按计划实施网络攻击行为
蓝方	防御方	在试验前制定防御计划,并部署防御技术。在试验过程中,防御攻击行为,保护目标系统



图4 想定生命周期
Figure 4 Scenario life cycle

1) 创建想定：主要由黄方完成，协调各方设计想定脚本。根据需求确定试验目标、规则、计划，确定参与人员信息、经济投入、潜在风险等。

2) 准备环境：主要由白方完成，包括设计网络拓扑、虚拟拓扑部署、数据采集配置、基础设施编排、漏洞注入、用户资源配置、访问控制等，绿方根据需求部署数据采集探针。

3) 排练检验：主要由黄方主导，测试试验环境，寻找可能的错误、漏洞和风险，确保流程执行正确、满足既定的规则等。

4) 想定执行：主要由各方参与，在CR中根据想定计划真实的运行试验活动。黄方负责流程控制，白方负责网络和资源管理与监控，绿方负责数据收集，红蓝方负责进行攻击和防御。

5) 分析评估：主要由绿方完成，收集必要数据，进行数据清理，利用机器学习等技术对试

验结果进行评估和分析，总结试验过程。

6) 想定结束：主要由白方完成，负责CR环境清理，进行数据归档、网络拓扑清除、资源释放等操作。

在想定脚本开发方面，试验过程中的各项配置可用脚本语言描述或利用图形化界面配置。想定脚本设计最常见的方式是采用描述语言，解析想定描述文件，为CR试验活动设置网络拓扑配置、漏洞注入、基础设施编排和资源配置等，规划CR活动的运作流程。

早期的想定设计方法主要基于YAML、XML、JSON等描述语言，具有代表性的CR项目包括CyTrONE、KYPO等。目前大部分CR基于OpenStack进行开发和建设，因此很多CR基于OpenStack自带的HEAT编排服务实现想定设计功能，其本质也是基于YAML文件生成模板。近年来，许多学者提出虚拟想定描述语言（virtual scenario design language, VSDL），并且利用Datalog、SMT等工具验证与测试想定脚本。这类自定义的想定脚本语言具有更强的可控性，但是想定设计需要技术门槛与业务知识，也增加了想定脚本语言的学习成本。想定脚本设计领域具有代表性的研究工作有CRACK、AIT、Cyber Arena等。近年来国外典型的想定设计工作对比如表15所示。

3.4.2 数据采集与评估

数据采集是指收集用户与CR交互的数据，如参赛选手生成的流量、使用的工具、获取的目标系统数据等。数据评估是指能够分析已采集数据，以了解CR的使用情况、用户执行情况等，分析参赛选手的行为以进行评分和排序，对部署的虚拟环境稳定性进行评估等。数据采集与评估方法取决于CR核心技术及模拟环境创建方式。

表 15 想定设计工作对比

Table 15 Comparison of scenario design works

工作	年份	核心思想总结	想定开发	基础设施
CyRIS ^[36] (开源)	2016	CyRIS 是 CyTrONE 环境的一部分, 使用 YAML 定义系统、部署软件和创建复制实例	YAML	OpenStack、KVM
KYPO ^[48] (开源)	2017	使用 YAML 构建想定, 把规格配置作为沙盒, 来协调底层基础设施配置, 规格利用 Ansible 语言来抽象构建指令	YAML	OpenNebula、OpenStack、Ansible
CRACK ^[49] (开源)	2020	基于 TOSCA 设计 SDL 想定设计语言, 能定义基础设施, SDL 转换成 Datalog 规范, 能支持验证, 验证后转换成 IaaS 供应商可识别的标准 IaC 指令	SDL 描述想定, Datalog 验证逻辑	OpenStack、SaC(想定即代码)
AIT ^[50]	2020	使用 TerraForm IaC 系统来部署 OpenStack 云基础设施	自定义基于 Web 的应用程序 GameMaker	OpenStack、Terraform、Ansible
Costa ^[51]	2020	设计 VSDL, 定义基础设施必须满足的约束条件。将约束提交给 SMT 求解器, 检查规范的可满足性。规范产生的模型将自动转换为要提交给 IaaS 提供商的部署 Packer 和 Terraform 脚本	VSDL 描述想定, SMT 验证检查	OpenStack、Terraform、Packer
CTL ^[52]	2020	基于模型驱动开发网络安全想定部署框架, 设计 CTL 描述系统的体系结构设置, 利用 Xtext 编写 CTL, 验证后转为 XML 再转为 HEAT, 能够检测网络配置问题和结构漏洞, 应用于 H2020 项目 THREAT-ARREST	网络安全训练语言 (CTL)	OpenStack、OpenStack Heat Template
Pierre ^[53]	2022	基于 Costa 等的工作, 设计 VSDL, 依赖基于特征的面向上下文的建模 FBCOP, 攻击-防御树中描述的显式用户档案和漏洞生成相关的 CR 想定	VSDL 和 FBCOP 描述想定, SMT 验证检查	OpenStack、Terraform、Packer
Yamin ^[54]	2022	使用 DSL(领域特定语言)构建想定, 能模拟漏洞、攻击、防御行为, 使用 BNF 书写规格, 使用 Datalog 进行想定验证	JSON 描述想定, BNF 和 Datalog 验证逻辑	OpenStack、OpenStack Heat Template
Cyber Arena ^[55] (开源)	2023	使用 YAML 定义想定。避免定义计算对象的软件和数据配置, 开发 IaC layer, 直接与云服务商交互, 获取云特征, 例如时延、DNS 等 IaC 标准中不能获取的数据	YAML	Google cloud、自定义 IaC

数据采集是 CR 试验的重要步骤, 支撑后续靶场试验成果分析等。在数据采集这一研究领域, 2018 年, Osaba 等^[56]针对室外可感知空间设计基于无线网络和 GPS 数据的数据采集系统, 包括真实的基础设施、数据采集系统和分析处理平台, 部署现实设备并对收集的网络数据进行分析。Tian 等^[57]基于 Heetian 网络靶场提出 C2RS 技术, 能获取靶场服务中主机级事件的实时相关性, 通过虚拟机自省技术实现带外数据获取和隔离。C2RS 将这些捕获的数据合并到波动性框架中, 以简化操作系统内存结构的分析。2019 年, 姚俊萍等^[58]针对当前网络数据采集时间长、质量低的问题, 分析采集结果时间序列的线性关系和变化趋势, 建立时间序列模型, 实现网络数据的多通道采集质量的高效、跨层控制。Tao 等^[59]针对工业网络物理系统设计信任数据方法, 用于事件检测的高质量数据收集, 兼顾效率与安全性能, 能够减轻传感器设备组

中积累的真实数据。根据应用程序需求, 减少传输到上游节点的数据量。Granasen 等^[60]在 2019 年“锁盾”网络防御演习中与蓝队一起收集指挥和控制、网络态势感知和情报等数据, 收集方式包括问卷调查、观察结果、团队沟通日志、分析报告和表现分数等。2020 年, Li 等^[61]针对 DNS 仿真中的数据采集问题, 提出一种轻加权主动数据收集方法, 为网络靶场内的 DNS 模拟准备数据集, 能够在短时间内收集 DNS 数据, 并具备较低的存储成本。

分析评估能够有助于增强靶场的可用性, 帮助改善想定设计, 提升靶场培训质量。2020 年, Andreolini 等^[62]提出靶场学员表现评估方法, 定义分布式监控体系结构, 收集学员活动相关信息; 使用有向图对学员活动进行建模; 基于图形操作的新评分算法评估学员表现, 能准确地衡量用户朝着目标前进的速度和准确率。Braghin 等^[63]针对 THREAT-ARREST 靶场, 提出模型驱

动的方法来监测和评估学员的表现,通过代理的系统来增强平台仿真环境,收集学员所执行的所有行为;提出模块化的动作分类法,可描述学员的预期行为,即正确执行练习所需的动作序列;利用有限状态机对学员的预期活动和实际活动进行建模,基于图匹配算法,根据图距离对学员表现进行评分。Erdogan等^[64]提出基于网络风险模型的靶场参与者网络安全技能评估方法,包括5个步骤:创建网络风险模型、识别风险治疗、设置培训场景、运行培训场景、评估参与者的表现。目标用户是白队和绿队。评估方法的输出是针对在靶场内接受培训的蓝队和红队的评估报告。2022年,Diakoumakos等^[65]设计联邦CR场景下的游戏化评分机制,指出联邦场景中所有节点需要有公共的评分模型、互相之间需要信息通信,并设计游戏模型的评分算法与公式。

3.4.3 靶场管理与监控

靶场管理通常是指靶场的导调层,负责编排和管理所有活动。靶场管理组件能够保障CR正常且高效运行^[66]。管理模块一般包括资源管理、角色管理、账号管理、流程管理等。监控功能模块可以看作靶场管理中的一部分功能,靶场监控是指对CR的状态进行实时把控,从而保障CR的正常运作。通常来说,CR管理员需要监控CR的运行状态、软硬件资源、网络流量、实时数据等。在CRATE、Cyber-SHIP、ECHO等项目中均设计靶场的管理与监控模块,通常管理与监控模块也是根据CR的需求定制的,是靶场正常运营不可缺少的组件。

在任务编排导调方面,2021年,Luise等^[67]针对基于云的CR提出动态部署、配置和导调框架,提出由多个交互部分组成的分布式架构,提供环境隔离、远程访问管理和控制、过程自动化、安全操作和可审计性。其中定义不同类型的资源,基于Amazon web服务和OpenVPN开发原型系统。2022年,Fu等^[68]提出一种无服务器容器的工作流编排方案,通过一个工作流模型来克服事件的异构性,该工作流模型使用组合DAG和统一的无服务器-容器事件触发器来编码事件链,该工作模型利用无服务器容器运行时代理来缩放调度工作流,实现CR导调。在管理监控方面,

2019年,Xie等^[69]针对CR中主机和客户系统之间的通信和控制需求,提出新的HSFT机制,提供与客户系统通信的网络连接,在读写速度上优于QGA守护进程程序。2021年,Terashima等^[70]发现在云环境上使用配置管理工具来构建靶场,能够提高靶场的可重复性和可扩展性,节约成本,但是步骤烦琐,因此提出KAKOI,利用自动化和模板化思想提供基础设计,简化用户构建靶场的步骤。

4 挑战与未来展望

4.1 挑战

CR经过多年发展,面临的技术挑战包括大规模网络仿真、海量网络攻击表达与检测、想定设计与开发。

(1) 大规模网络仿真

现实的网络系统具有随机性、动态性、复杂性等特点,真实大规模网络系统中各种事件往往随机发生、数据流动频繁、网络结构复杂^[71]。例如,在军事网安演习中需要模拟大规模军事网络环境,涵盖多个作战单元和指挥中心。这类仿真需要高度逼真的网络环境。在智慧城市CR中,需要模拟各种关键基础设施系统和大规模复杂城市网络^[72]。CR仿真技术发展多年,仍存在难以解决的问题。

1) 特殊对象仿真:CR难以完全复现某些特殊对象,部分专用网络系统包含未公开的专用设备和特殊部件,由于厂商技术保密等因素,这些特殊对象难以仿真,通常只能用真实设备代替。另外,针对未知的网络系统缺陷和漏洞,靶场也难以进行仿真。

2) 大规模网络仿真:现有技术难以实时、准确仿真超大规模复杂网络,CR面临大量数据实时计算的性能瓶颈、海量数据的快速和可靠存储压力、异构和动态复杂网络建模困难等挑战。

(2) 海量网络攻击表达和检测

全球已知的亿种网络攻击不断演化,针对海量的网络攻击如何做到清晰、全面的知识表达以及准确、实时的攻击检测是世界性难题^[73]。网络攻击具有多点性(攻击者可从各脆弱节点入手逐步攻击)、多层性(攻击可分布在物理层、网络层、控制层等)、多类性(不同设备的攻击类

型异构)[74]。CR 中各种试验场景、网络层次、仿真设备众多,面对 3 种特性相互耦合关联的各种攻击,难以做到海量攻击表达与检测。

1) 网络攻击知识难以表达:现有网络攻击知识规模巨大且不断演化,存在着多维关联和时空特性,难以用传统的知识表达和管理方法进行描述。CR 中管理网络攻击知识还需要额外设计庞大的攻击知识库以及对应的知识解析方法。

2) 难以准确高效检测攻击:CR 在运行过程中存在着大量的无效攻击且现有安全防护机制误报率高,如何从海量无效攻击中快速、准确识别出真实有效的网络攻击是当今 CR 攻击检测技术面临的挑战。有些网络攻击链路复杂,现有靶场难以准确、快速地展示多步攻击链路。

(3) 想定设计与开发

想定设计是目前国内外差别较大的领域,其目标是最小化演习生命周期中每个阶段需要的人力投入[75]。国外想定设计开发工作处于快速发展与应用阶段,国内想定设计开发处于起步阶段,较少 CR 实现基于想定的自动化配置,大部分 CR 需要人工配置试验活动的各种细节。目前国内 CR 想定设计与开发工作仍面临以下挑战。

1) 设计思路:由于 CR 具有军事用途特性,很多技术细节保密,难获取各国大型 CR 平台技术信息。国内想定设计主要是参考国外学术研究成果,大部分用于网安演练和培训,其设计思路不一定符合实际 CR 需求,暂时没有满足不同应用场景、不同 CR 架构等的通用想定设计思路。

2) 技术挑战:想定设计主要基于脚本语言以及各种 IaC 工具(Terraform、Ansible、Chef 等),国内 CR 实现想定功能时需适配不同的技术栈,如有些 CR 底层基于私有云或专用基础设施,难以使用现成工具进行配置和管理,难以开发具有可扩展性和通用性的想定模块。

4.2 未来展望

未来网络靶场设想如图 5 所示,CR 建设有望在 3 个方面取得进展。

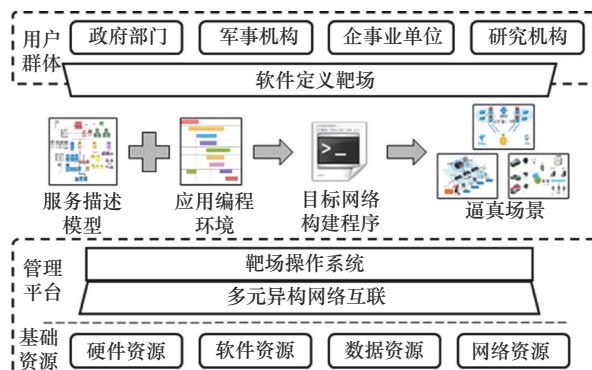


图 5 未来网络靶场设想

Figure 5 Future vision of cyber ranges

(1) 体系结构方面

1) 联邦靶场:早期的 CR 多为单一的集中式靶场,随着网络规模飞速发展,近年涌现许多联邦靶场项目,以实现跨物理区域的资源互联和共享。未来建立联邦靶场是一大趋势,通过连接各城市、各行业的 CR,可以构建一个更真实、更复杂的国家级虚拟网络环境,从而应对未来潜在的网络风险。通过与其他国家合作,建立跨国 CR,能够加强技术合作,促进全球网络安全研究发展。在建设联邦靶场过程中,也需要进行技术升级和创新,促进行业融合。

2) 靶场即服务:随着靶场技术不断发展,未来将出现靶场即服务[66]。用户可以像用水、用电一样方便灵活、自主定义专有的靶场服务。网络靶场作为网络安全研究基础设施,将以云计算服务的形式,提供靶场服务平台,使用户能够部署、运行、管理和扩展专用目标网络环境和攻防演练场景。CR 提供分布式资源虚拟化能力,以及人、机、物互联能力,使开发者可以专注于应用场景的设计和部署,而不必关注底层基础设施的管理。同时未来 CR 将提供一系列工具和服务,如服务描述模型、应用编程环境、目标网络构建程序等。

(2) 应用领域方面

1) 人工智能:近年来,以 ChatGPT 为代表的大模型技术吸引了全球的目光,其具备对话、数学计算推理、代码编写等能力,成为新一轮的计算机技术发展热点。AI 安全性也备受瞩目,未来将出现面向 AI 场景的 CR,保障 AI 技术安全。另外,将 AI 技术应用到靶场也存在

许多潜在发展方向, 包括智能化攻防模拟工具、智能化培训教育服务、靶场智能管理模式等。

2) 新型行业: CR的应用领域将不再局限于传统行业, 如电力、金融、工业控制等。新的应用领域同样需要建设CR, 如航空航天、卫星、智慧城市等领域。随着特殊应用场景的出现, 未来可结合现有靶场技术和新型领域专业需求, 建设专用领域靶场, 满足新应用行业的需求。

(3) 关键技术方面

1) 靶场操作系统: 目前的靶场大部分是基于操作系统构建的应用程序, 通常以客户端或浏览器形式提供服务。这种方式对用户友好、具备较高的兼容性, 但是存在着可控性较差、管理监控不便等问题。未来的靶场操作系统将满足靶场内部数据管理、状态监控等需求, 支撑底层分布式资源的统一管理和虚拟化, 以及可编程的靶场业务开发平台, 为用户提供定制化网络试验场景。

2) 靶场关键技术: 在网络仿真技术方面, 未来的模拟仿真技术将愈发成熟, 支撑大规模复杂网络仿真, 基于容器的虚拟化技术将更多应用于CR, 针对现实复杂应用系统的安全评测也将更加完善。随着技术升级, 越来越多的CR会开始关注想定设计、开发、管理等领域^[21]。在攻击检测技术方面, 未来会与大数据技术结合, 实现高效、准确的网络攻击检测, 增强CR安全防护能力。

5 结束语

本文聚焦网络靶场, 首先梳理4个发展阶段, 从2个维度对靶场进行分类; 接着介绍典型的靶场架构; 然后分析国内外靶场研究现状, 在工业界方面, 调研超30个靶场项目, 总结各国典型靶场, 在学术界方面, 介绍靶场经典综述工作、靶场关键技术研究、靶场建设框架; 最后指出当前靶场建设面临的挑战, 展望未来靶场体系结构、应用领域、关键技术的发展趋势。本文工作期望能够为国内网络靶场研究提供技术参考与创新启示。

参考文献:

- [1] 方滨兴. 定义网络空间安全[J]. 网络与信息安全学报, 2018, 4(1): 1-5.
FANG B X. Define cyberspace security[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 1-5
- [2] 李馥娟, 王群. 网络靶场及其关键技术研究[J]. 计算机工程与应用, 2022, 58(5): 12-22.
LI F J, WANG Q. Research on cyber ranges and its key technologies[J]. Computer Engineering and Applications, 2022, 58(5): 12-22.
- [3] 方滨兴, 贾焰, 李爱平, 等. 网络空间靶场技术研究[J]. 信息安全学报, 2016, 1(3): 1-9.
FANG B X, JIA Y, LI A P, et al. Cyber ranges: state-of-the-art and research challenges[J]. Journal of Cyber Security, 2016, 1(3): 1-9.
- [4] FERGUSON B, TALLA, OLSEND. National cyber range overview[C]// Proceedings of the 2014 IEEE Military Communications Conference. Piscataway: IEEE Press, 2014: 123-128.
- [5] NIST Cyber Range Project Team and the NICE Community. The cyber range: a guide[R]. 2023.
- [6] European Cyber Security Organisation (ECSSO). Understanding cyber ranges: from hype to reality[R]. 2020.
- [7] UKWANDU E, FARAH M A B, HINDY H, et al. A review of cyber-ranges and test-beds: current and future trends[J]. Sensors, 2020, 20(24): 7148.
- [8] 李宁, 刘俊, 张君, 等. 2023年全球网络演习概览[J]. 信息安全与通信保密, 2024, 22(1): 26-33.
LI N, LIU J, ZHANG J, et al. Overview of the global cyber exercise in 2023[J]. Information Security and Communications Privacy, 2024, 22(1): 26-33.
- [9] 李伦, 王曦, 郝志宇. 美国网络空间靶场建设情况综述[J]. 保密科学技术, 2021(6): 53-60.
LI L, WANG X, HAO Z Y. A summary of the construction of cyberspace shooting range in the United States[J]. Secrecy Science and Technology, 2021(6): 53-60.
- [10] 李秋香, 郝文江, 李翠翠, 等. 国外网络靶场技术现状及启示[J]. 信息网络安全, 2014(9): 63-68.
LI Q X, HAO W J, LI C C, et al. Present situation and enlightenment of the foreign network range technology[J]. Netinfo Security, 2014(9): 63-68.
- [11] CARY D. Downrange: a survey of china's cyber ranges[J]. Center for Security and Emerging Technology, September, 2022.
- [12] 陈丽, 段红, 李革. 大数据技术在网络靶场中的发展趋势研究[C]//第24届中国系统仿真技术及其应用学术年会论文集. 合肥, 2023: 111-115.
CHEN L, DUAN H, LI G. Research on the development trend of big data technology in cyber range[C]//CCSSTA 24th 2023, Hefei, 2023: 111-115.
- [13] 李冬, 于俊清, 谷永普, 等. 高效安全的软件定义网络拓扑发现协议[J]. 网络与信息安全学报, 2023, 9(6): 20-33.
LI D, YU J Q, GU Y P, et al. Efficient and safe software defined network topology discovery protocol[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 20-33.

- [14] 王佰玲, 刘红日, 张耀方, 等. 工业控制系统安全仿真关键技术研究综述[J]. 系统仿真学报, 2021, 33(6): 1466-1488.
WANG B L, LIU H R, ZHANG Y F, et al. Review on key technologies of industrial control system security simulation[J]. Journal of System Simulation, 2021, 33(6): 1466-1488.
- [15] 张淼, 许凯, 彭勇, 等. 建模与仿真服务化研究综述[J]. 自动化学报, 2023, 49(8): 1601-1620.
ZHANG M, XU K, PENG Y, et al. Overview of servitization of modeling and simulation[J]. Acta Automatica Sinica, 2023, 49(8): 1601-1620.
- [16] 邱志明, 李恒, 周玉芳, 等. 模拟仿真技术及其在训练领域的应用综述[J]. 系统仿真学报, 2023, 35(6): 1131-1143.
QIU Z M, LI H, ZHOU Y F, et al. Summary of simulation technology and its application in training field[J]. Journal of System Simulation, 2023, 35(6): 1131-1143.
- [17] DAVIS J, MAGRATH S. A survey of cyber ranges and testbeds[R]. 2013.
- [18] HOLM H, KARRESAND M, VIDSTRÖM A, et al. A survey of industrial control system testbeds[M]. Secure IT Systems: vol 9417. Cham: Springer, 2015: 11-26.
- [19] VYKOPAL J, VIZVARY M, OSLEJSEK R, et al. Lessons learned from complex hands-on defence exercises in a cyber range[C]//Proceedings of the 2017 IEEE Frontiers in Education Conference (FIE). Piscataway: IEEE Press, 2017: 1-8.
- [20] PRIYADARSHINI I. Features and architecture of the modern cyber range: a qualitative analysis and survey[D]. Newark: University of Delaware, 2018.
- [21] YAMIN M M, KATT B, GKIOULOS V. Cyber ranges and security testbeds: scenarios, functions, tools and architecture[J]. Computers & Security, 2020, 88: 101636.
- [22] CHOULIARAS N, GEORGE K, IOANNA K, et al. Cyber ranges and TestBeds for education, training, and research[J]. Applied Sciences, 2021, 11(4): 1809.
- [23] GLAS M, VIELBERTH M, PERNUL G. Train as you fight: evaluating authentic cybersecurity training in cyber ranges[C]//Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. New York: ACM, 2023: 1-19.
- [24] VYRON K, GKIOULOS V, KATSIKAS S. A systematic literature review on wireless security testbeds in the cyber-physical realm[J]. Computers & Security, 2023, 133: 103383.
- [25] 符永铨, 赵辉, 王晓锋, 等. 网络行为仿真综述[J]. 软件学报, 2022, 33(1): 274-296.
FU Y Q, ZHAO H, WANG X F, et al. State-of-the-art survey on network behavior emulation[J]. Journal of Software, 2022, 33(1): 274-296.
- [26] LEBLANC S P, PARTINGTON A, CHAPMAN I, et al. An over-view of cyber attack and computer network operations simulation[C]//Proceedings of the 2011 Military Modeling & Simulation Symposium, 2011: 92-100.
- [27] WEHRLE K, GÜNEŞ M, GROSS J. Modeling and tools for network simulation[M]. Berlin: Springer, 2010.
- [28] GOMEZ J, KFOURY E F, CRICHIGNO J, et al. A survey on network simulators, emulators, and testbeds used for research and education[J]. Computer Networks, 2023, 237: 110054.
- [29] LIU C H, YAN W, XU F K, et al. User behavior simulation in ICS cyber ranges[C]//Proceedings of the 2022 19th Annual International Conference on Privacy, Security & Trust (PST). Piscataway: IEEE Press, 2022: 1-5.
- [30] 吴佩翔, 张志龙, 陈力波, 等. 针对 5G 核心网协议的自动化漏洞挖掘方法[J]. 网络与信息安全学报, 2024, 10(1): 156-168.
WU P X, ZHANG Z L, CHEN L B, et al. Automated vulnerability discovery method for 5G core network protocol[J]. Chinese Journal of Network and Information Security, 2024, 10(1): 156-168.
- [31] MOSKAL S, YANG S J, KUHL M E. Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach[J]. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 2018, 15(1): 13-29.
- [32] PAN W Q, LIU X H, HAN J, et al. Scorpio: an automated penetration testing tool and its integration with a cyber range[C]//Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT). Piscataway: IEEE Press, 2021: 1113-1119.
- [33] JIANG H T, CHOI T, KO R K L. Pandora: a cyber range environment for the safe testing and deployment of autonomous cyber attack tools[C]//International Symposium on Security in Computing and Communication. Singapore: Springer, 2021: 1-20.
- [34] ANTONOPOULOS M, DRAINAKIS G, OUZOUNOGLU E, et al. Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain[C]//Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR). Piscataway: IEEE Press, 2022: 305-310.
- [35] 段红, 邱晓刚. 网络化仿真及其发展趋势[J]. 系统仿真学报, 2021, 33(7): 1526-1533.
DUAN H, QIU X G. Networked simulation and it's development trend[J]. Journal of System Simulation, 2021, 33(7): 1526-1533.
- [36] PHAM C, TANG D, CHINEN K I, et al. CyRIS: a cyber range instantiation system for facilitating security training[C]//Proceedings of the Seventh Symposium on Information and Communication Technology. New York: ACM, 2016: 251-258.
- [37] SCHOONOVER K, MICHALAK E, HARRIS S, et al. Galaxy: a network emulation framework for cyber security[C]//Proceedings of 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18). 2018.
- [38] CHEN Y, ZHANG G J, HU D L, et al. Multiscale emulation technology based on the integration of virtualization, physical and simulation networks[C]//Proceedings of the 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2019: 396-402.
- [39] 刘渊, 邱常伶, 王晓锋, 等. 面向多尺度融合网络仿真的拓扑映射方法研究[J]. 系统仿真学报, 2019, 31(10): 2030-2041.
LIU Y, QIU C L, WANG X F, et al. Research on topology mapping method for multiscale integration network emulation[J]. Journal of System Simulation, 2019, 31(10): 2030-2041.

- [40] 王晓锋, 谌泰乾, 刘渊. 面向卫星互联网的动态仿真技术研究[J]. 系统仿真学报, 2023, 35(7): 1472-1486.
WANG X F, CHEN T Q, LIU Y. Research on dynamic simulation technology for satellite Internet[J]. Journal of System Simulation, 2023, 35(7): 1472-1486.
- [41] ADELEKE O A, BASTIN N, GURKAN D. Network traffic generation: a survey and methodology[J]. ACM Computing Surveys, 2023, 55(2): 1-23.
- [42] JAVALI C, REVADIGAR G. Network web traffic generator for cyber range exercises[C]//Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN). Piscataway: IEEE Press, 2019: 308-315.
- [43] 李松, 周亚同, 池越, 等. 高斯过程混合模型应用于网络流量预测研究[J]. 计算机工程与应用, 2020, 56(5): 186-193.
LI S, ZHOU Y T, CHI Y, et al. Application of Gaussian process mixture model on network traffic prediction[J]. Computer Engineering and Applications, 2020, 56(5): 186-193.
- [44] LEE C. Method for providing background traffic using IP random assigning in cyber range[J]. Electronics Letters, 2021, 57(6): 261-263.
- [45] DU L F, HE J J, LI T, et al. DBWE-Corbat: background network traffic generation using dynamic word embedding and contrastive learning for cyber range[J]. Computers & Security, 2023, 129: 103202.
- [46] HUANG X, WANG X F, LIU Y, et al. A distributed traffic replay framework for network emulation[J]. Information, 2023, 14(2): 59.
- [47] 王进文, 张晓丽, 李琦, 等. 网络功能虚拟化技术研究进展[J]. 计算机学报, 2019, 42(2): 185-206.
WANG J W, ZHANG X L, LI Q, et al. Network function virtualization technology: a survey[J]. Chinese Journal of Computers, 2019, 42(2): 185-206.
- [48] ČELEDÁ P, ČEGAN J, VYKOPAL J, et al. Kypo - a platform for cyber defence exercises[J]. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. 2015.
- [49] RUSSO E, COSTA G, ARMANDO A. Building next generation cyber ranges with CRACK[J]. Computers & Security, 2020, 95: 101837.
- [50] LEITNER M, FRANK M, HOTWAGNER W, et al. AIT cyber range: flexible cyber security environment for exercises, training and research[C]//Proceedings of the European Interdisciplinary Cybersecurity Conference. New York: ACM, 2020: 1-6.
- [51] COSTA G, RUSSO E, ARMANDO A. Automating the generation of cyber range virtual scenarios with VSDL[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2022, 13(4): 61-80.
- [52] BRAGHIN C, CIMATO S, DAMIANI E, et al. A model driven approach for cyber security scenarios deployment[M]. Computer Security. Cham: Springer International Publishing, 2020: 107-122.
- [53] MARTOU P, MENS K, DUHOUX B, et al. Generating virtual scenarios for cyber ranges from feature-based context-oriented models: a case study[C]//Proceedings of the 14th ACM International Workshop on Context-Oriented Programming and Advanced Modularity. New York: ACM, 2022: 35-43.
- [54] YAMIN M M, KATT B. Modeling and executing cyber security exercise scenarios in cyber ranges[J]. Computers & Security, 2022, 116: 102635.
- [55] KARJALAINEN M, KOKKONEN T. Comprehensive cyber arena; the next generation cyber range[C]//Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Piscataway: IEEE Press, 2020: 11-16.
- [56] OSABA E, PIERDICCIA R, MALINVERNI E, et al. A smartphone-based system for outdoor data gathering using a wireless beacon network and GPS data: from cyber spaces to senseable spaces[J]. ISPRS International Journal of Geo-Information, 2018, 7(5): 190.
- [57] TIAN Z H, CUI Y, AN L, et al. A real-time correlation of host-level events in cyber range service for smart campus[J]. IEEE Access, 2018, 6: 35355-35364.
- [58] 姚俊萍, 范守祥, 李晓军. 网络数据多通道采集质量跨层控制方法仿真[J]. 计算机仿真, 2019, 36(10): 289-292.
YAO J P, FAN S X, LI X J. Simulation of multi-channel acquisition quality cross-layer control method for network data[J]. Computer Simulation, 2019, 36(10): 289-292.
- [59] TAO H, BHUIYAN M Z A, RAHMAN M A, et al. TrustData: trustworthy and secured data collection for event detection in industrial cyber-physical system[J]. IEEE Transactions on Industrial Informatics, 2020, 16(5): 3311-3321.
- [60] GRANÅSEN M, HUSKAJ G, VARGA S. Data collection and research in CDXs: command and control, cyber situational awareness and intelligence perspectives on cyber defense[C]//Proceedings of 24th International Command and Control Research and Technology Symposium (ICCRTS), USA: International Command and Control Institute, 2019.
- [61] LI S, DU S, HUANG W, et al. A light-weighted data collection method for DNS simulation on the cyber range[J]. KSII Transactions on Internet and Information Systems, 2020, 14(8): 3501-3518.
- [62] ANDREOLINI M, COLACINO V G, COLAJANNI M, et al. A framework for the evaluation of trainee performance in cyber range exercises[J]. Mobile Networks and Applications, 2020, 25(1): 236-247.
- [63] BRAGHIN C, CIMATO S, DAMIANI E, et al. Towards the monitoring and evaluation of trainees' activities in cyber ranges[C]. International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity. Cham: Springer, 2020: 79-91.
- [64] ERDOGAN G, HUGO Á, ROMERO A, et al. An approach to train and evaluate the cybersecurity skills of participants in cyber ranges based on cyber-risk models[C]//Proceedings of the 15th International Conference on Software Technologies. SCITEPRESS - Science and Technology Publications, 2020: 509-520.
- [65] DIAKOUMAKOS J, CHASKOS E, KOLOKOTRONIS N, et al. Cyber-range federation and cyber-security games: a gamification scoring model[C]//Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Piscataway: IEEE Press, 2021: 186-191.
- [66] ORBINATO V. A next-generation platform for cyber range-as-a-

- service[C]//Proceedings of the 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). Piscataway: IEEE Press, 2021: 314-318.
- [67] LUISE A P, PERRONE G, PERROTTA C, et al. On-demand deployment and orchestration of cyber ranges in the cloud[C]//ITASEC. 2021: 80-91.
- [68] FU Y Q, HAN W H, YUAN D. Orchestrating heterogeneous cyber range event chains with Serverless-container workflow[C]//Proceedings of the 2022 30th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). Piscataway: IEEE Press, 2022: 97-104.
- [69] XIE J J, ZHANG C R, LOU F, et al. High-speed file transferring over linux bridge for QGA enhancement in cyber range[C]//International Conference on Artificial Intelligence and Security. Cham: Springer, 2019: 452-462.
- [70] TERASHIMA T, NAKAYAMA M, YOKOYAMA T, et al. KAKOI: a new tool to make simple and secure build cyber ranges using public cloud[C]//Proceedings of the 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW). Piscataway: IEEE Press, 2021: 398-404.
- [71] GU Z. MDATA: a new knowledge representation model: theory, methods and applications[M]. Cham: Springer, 2021.
- [72] DEMERTZI V, DEMERTZIS S, DEMERTZIS K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities[J]. Applied Sciences, 2023, 13(2): 790.
- [73] JIA Y, GU Z Q, DU L, et al. Artificial intelligence enabled cyber security defense for smart cities: a novel attack detection framework based on the MDATA model[J]. Knowledge-Based Systems, 2023, 276: 110781.
- [74] DU D J, ZHU M G, LI X, et al. A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems[J]. Journal of Modern Power Systems and Clean Energy, 2023, 11(3): 727-743.
- [75] VYKOPAL J, OŠLEJŠEK R, ČELEDÁ P, et al. KYPO cyber range: design and use cases[C]//International Conference on Software Technologies (ICSOFT'17). 2017: 310-321.

[作者简介]:



邹星 (1994-), 女, 湖北荆州人, 鹏城实验室助理工程师, 主要研究方向为网络空间安全、网络靶场、云计算。



胡宁 (1972-), 男, 湖南长沙人, 鹏城实验室研究员、博士生导师, 主要研究方向为网络空间安全、工业控制系统安全、软件定义网络与网络虚拟化。



顾钊铨 (1989-), 男, 四川巴中人, 哈尔滨工业大学(深圳)教授, 鹏城实验室研究员、博士生导师, 主要研究方向为网络靶场、网络攻击研判、人工智能安全。



贾焰 (1960-), 女, 四川成都人, 鹏城实验室研究员、博士生导师, 主要研究方向为网络空间安全、大数据分析和人工智能。