ICS 35.030
CCS L67

# 中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

# 网络安全技术 网络安全试验平台 互联互通指南

Cybersecurity techniques — Cybersecurity experiment platform — Interconnection guidelines

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

国家市场监督管理总局
国家标准化管理委员会 发布

# 目　　次

前言 …… III
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号与缩略语 …… 2
5　网络安全试验平台互联 …… 2
5.1　概述 …… 2
5.2　互联架构 …… 2
5.3　互联模型 …… 4
6　互联互通 …… 5
6.1　基础网络互联 …… 5
6.2　业务数据互联 …… 6
c)　资源控制互联 …… 7
c)　业务管理互联 …… 7
附录 A（资料性）　通过互联四个层次协同完成试验的示例 …… 9
附录 B（资料性）　异构靶场互联参考 …… 10
参考文献 …… 11

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：鹏城实验室、广州大学、国家计算机网络应急技术处理协调中心、哈尔滨工业大学（深圳）、中国移动通信集团有限公司、中国联合网络通信有限公司广州市分公司、中国电信股份有限公司研究院、北京航天万源科技有限公司、航天通信中心、广东电网有限责任公司广州供电局、北京邮电大学、中国工商银行股份有限公司、中国联合网络通信有限公司研究院、中国第一汽车股份有限公司研发总院、中石化安全工程研究院有限公司、中国融通安防国际集团有限公司、博智安全科技股份有限公司、中国电子信息产业集团有限公司第六研究所、国汽（北京）智能网联汽车研究院有限公司、中国汽车技术研究中心有限公司、中汽智能科技（天津）有限公司、中汽创智科技有限公司、中国汽车工程研究院股份有限公司、中国信息通信研究院、南方电网科学研究院有限责任公司、国网江西省电力有限公司信息通信分公司、春天研究院（深圳）有限公司、软极网络技术(北京)有限公司、四川亿览科技股份有限公司、内蒙古工业大学、内蒙古电力（集团）有限责任公司、内蒙古大唐国际托克托发电有限责任公司、深圳市燃气集团股份有限公司、深圳市政务服务和数据管理局、山东省计算中心(国家超级计算济南中心)、启明星辰信息技术集团股份有限公司、山东乾云启创信息科技股份有限公司、招商局船舶工业智能科技（江苏）有限公司、北京丁牛科技有限公司、永信至诚科技集团股份有限公司、杭州安恒信息技术股份有限公司、南京赛宁信息技术有限公司、国核自仪系统工程有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司、中移互联网有限公司、中科信息安全共性技术国家工程研究中心有限公司、广东为辰信息科技有限公司、中电长城网际安全技术研究院、联通智网科技股份有限公司、明阳产业技术研究院（沈阳）有限责任公司、中山市政务服务数据管理局、广州锦行网络科技有限公司、广西数广威奇科技有限公司、北京六方云信息技术有限公司、四川铁道职业学院、东莞中科云计算研究院、数字广西集团有限公司。

本文件主要起草人：贾焰、胡宁、李树栋、顾钊铨、韩伟红、田志宏、刘欣然、侯路、王帅、郑轶、杨连成、吴晓波、张军、殷丽华、胡尧、钟国新、王辉鹏、季万松、董航、张晨、徐雷、蒋家堂、崔牧凡、安伦、李润恒、赵大伟、续焕超、林汝梁、梁志宏、刘凯、刘居佳、胡建勋、王龑、冀甜甜、孙岩炜、王忠杰、肖岩军、胡斌、杨鑫、孙琦、曹德舜、蔡晶晶、靳子辉、高翔、吴瑞、任宽、黄恩兴、王凯民、刘建辉、王钢、郭琦、奥伟、孙布勒、暴田双、陶莎、周逸菲、邱浚漾、唐焯宜、苗春雨、叶帅辰、关墨辰、谢敏容、包华宇、方锐、秦孔建、贺可勋、杨彦召、贺鹏、郭韬、李维皓、周艳、周光涛、邱日轩、赵焕宇、张大海、关宝锵、周舟、黄海军、苗雷、达少辉、张丹毅。

# 网络安全技术 网络安全试验平台 互联互通指南

## 1 范围

本文件给出了网络安全试验平台互联互通的建设指南，包括基础网络互联、业务数据互联、资源控制互联、业务管理互联四个互联层次的能力、管理和安全建议。

本文件适用于网络安全试验平台之间互联业务。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 36968—2018 信息安全技术 IPSec VPN 技术规范

GB/T 46820—2025 网络安全技术 网络安全试验平台 体系架构

YD/T 4587—2023 网络空间安全仿真术语

## 3 术语和定义

GB/T 25069-2022、GB/T 36968-2018、GB/T 46820-2025、YD/T 4587-2023 界定的以及下列术语和定义适用于本文件。

3.1

**网络空间安全仿真 cybersecurity emulation**

通过虚拟环境与真实设备相结合，模拟仿真出真实网络空间攻防环境，能够支撑网络空间攻防能力研究和网络空间攻防工具验证试验平台。

3.2

**网络安全试验平台 cybersecurity emulation platform**

一种大型网络仿真测试平台，为网络安全技术和产品提供评估，为网络安全培训和实验提供安全可控的设施，为模拟真实的网络攻防提供虚拟环境。

3.3

**分布式网络安全试验平台 distributed range**

由多个分散在不同地点的独立的网络安全试验平台构成,这些独立的网络安全试验平台不共享硬件设备,它们通过网络安全试验平台所基于的通信网络发送和接收数据进行合作以共同执行和完成任务。

3.4

**目标网络构建方 target network builder**

网络安全试验平台中目标网络的构建和维护者。

# 4 符号与缩略语

下列符号适用于本文件。

BGP：边界网关协议（Border Gateway Protocol）

ISIS：中间系统到中间系统（Intermediate system to intermediate system）

MPLS：多协议标签交换（Multiprotocol Label Switching）

OSPF：开放式最短路径优先（Open Shortest Path First）

QoS：服务质量（Quality of Service）

TCP/IP：传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol）

VPN ：虚拟专用网络（Virtual Private Network）

VxLAN：虚拟可扩展局域网（Virtual eXtensible Local Area Network）

WAN：广域网（Wide Area Network）

# 5 网络安全试验平台互联

## 5.1 概述

网络安全试验平台互联互通，即要解决两个或多个异构网络安全试验平台，因其数据格式、通信协议、组成结构、资源类型、业务能力、安全防护等方面不同造成的无法共享资源的问题。通过网络安全试验平台互联互通，即可将多个网络安全试验平台组合到一起，开展统一调度、统一控制的联合试验，以形成分布式网络安全试验平台。互联互通克服单一网络安全试验平台在资源和能力方面的局限性，通过试验平台间资源共享，实现仿真的逼真度及资源利用率的提升，增强具有领域特色的网络安全试验平台，包括互联网网络安全试验平台、电力网络安全试验平台、汽车网络安全试验平台等各领域试验平台间的协同，从而更真实的复现真实环境的复杂性。

网络安全试验平台的互联架构包括：集中式互联和分布式互联两种架构，用于满足不同类型的网络空间安全仿真需求。

## 5.2 互联架构

### 5.2.1 集中式互联

主网络安全试验平台是集中式互联架构的核心，负责分网络安全试验平台之间的互通和资源协调。分网络安全试验平台提供领域特色的靶标资源。

集中式互联，通过主试验平台实现分平台的管理，包括接入管理，资源管理，分平台之间网络互通等，同时通过对不同网络安全试验平台计算资源、存储资源和网络资源的互操作、可重用和可组合，实现一个主网络安全试验平台和多个分网络安全试验平台的资源共享。

如图 1 所示。在集中式互联架构中，主网络安全试验平台作为汇聚节点同时连接多个不同类型的分网络安全试验平台，为不同的分网络安全试验平台提供数据交换和协议适配服务，实现网络环境扩展、资源共享和互操作，分网络安全试验平台之间没有直接互联关系。

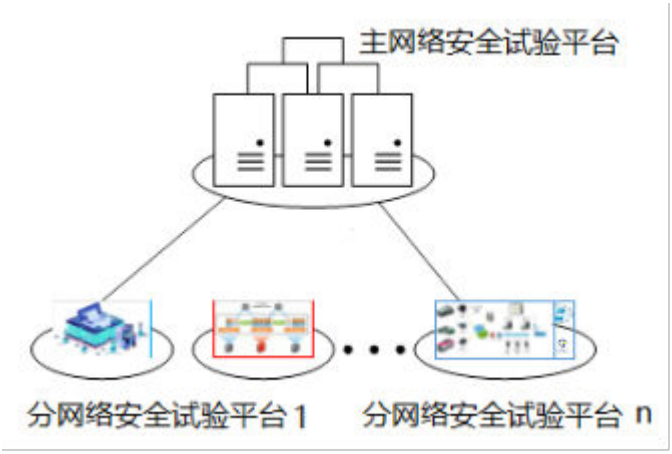



图 1 集中式互联

### 5.2.2 分布式互联

分布式互联用于多个彼此独立运行的网络安全试验平台之间，通过互联网络实现远程互联，以此实现网络环境扩展、资源共享和互操作。

分布式互联架构如图 2 所示。

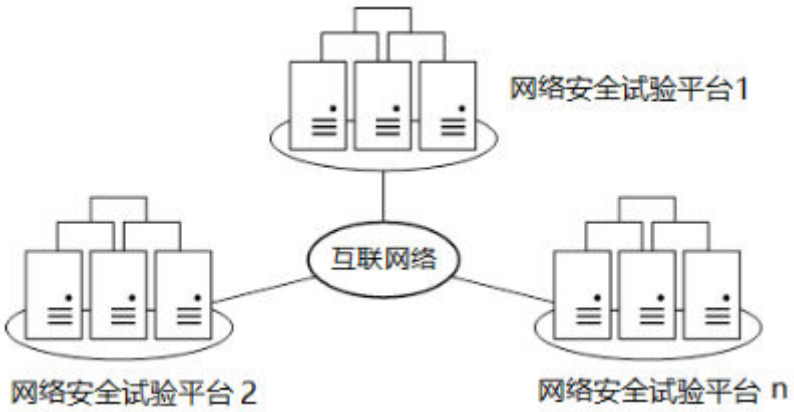



图 2 分布式互联

其中，在点对点互联架构下，

a) 如图 3 所示，单一、小规模的网络安全试验平台之间的通过专线，互联网 VPN 等方式实现互联。

b) 如图 4 所示，实物设备通过 IP 网络或者物理线路远程接入目标网络安全试验平台，作为网络安全试验平台的组成部分供用户访问，实物设备仅需提供基本的远程访问能力。

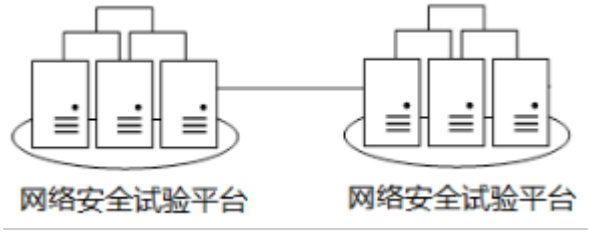


图 3 试验平台之间互联

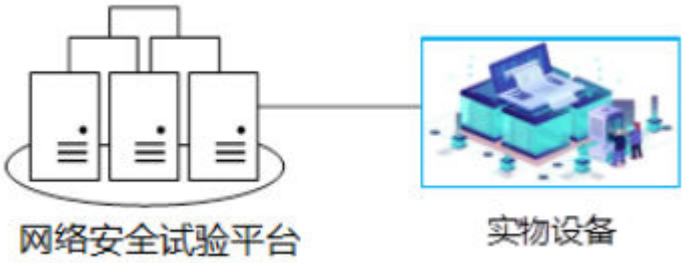



图 4 试验平台与实物靶标互联

特别的，点对点互联做为分布式互联的特例，主要用于支撑单一、小规模的网络安全试验平台之间的互联，或者实物靶标接入到网络安全试验平台。

## 5.3 互联模型

### 5.3.1 互联模型组成

根据 GB/T46820—2025 7.5 中描述，按照互联的能力水平从低到高，网络安全试验平台互联模型从基础网络互联、业务数据互联、资源控制互联和业务管理互联四个层次描述互联业务需求。

如图 5 所示，网络安全试验平台互联模型描述了不同网络安全试验平台互联过程中所涉及到的逻辑模块和不同的互联层次。

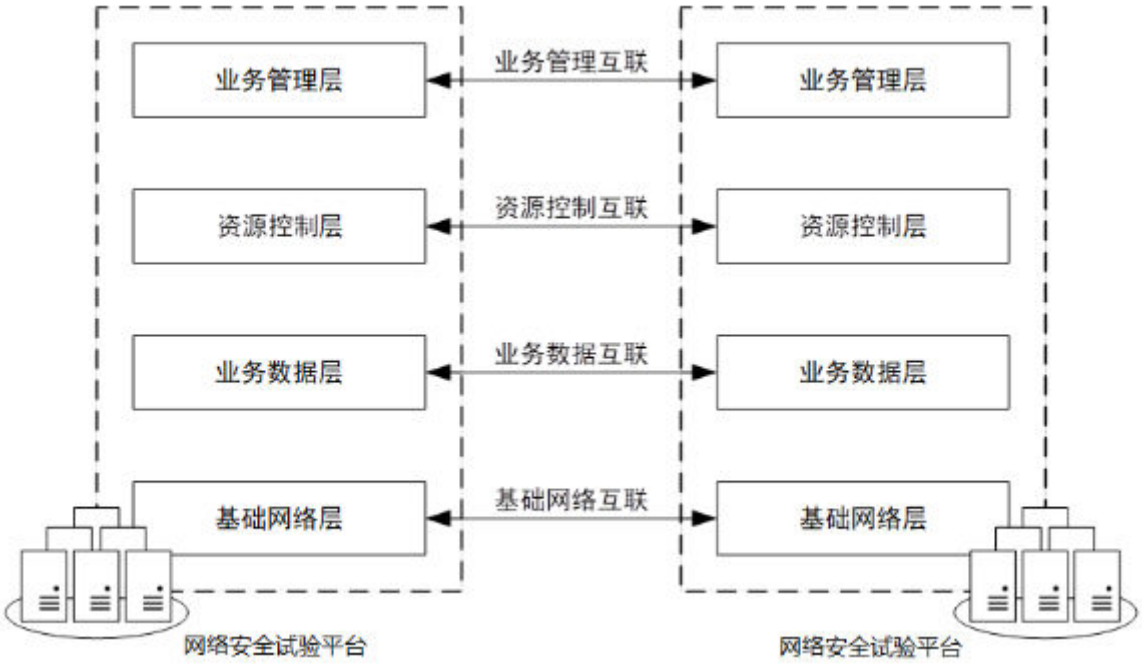



图 5 网络安全试验平台互联模型

### 5.3.2 基础网络层

基础网络层包括：基础硬件平台和系统软件。基础网络层基于 TCP/IP 网络实现互联、互通，可基于 IP 分组进行数据交换，可基于 BGP、OSPF、ISIS 等路由协议进行路由交换。基础网络层的互联互通是实现网络安全试验平台之间仿真互联的基本能力。

### 5.3.3 业务数据层

为保证业务数据在基于公共网络环境（如：MPLS VPN、互联网、5G、无线网络等）中构建的实现基础网络层中传输不受影响，需采取特定的隧道协议对业务数据流进行封装。因此，在 IP 数据平面的基础上定义业务数据层，将业务数据流按照特定的格式进行封装，并作为 IP 分组的应用载荷进行传输。业务数据层定义了业务数据流的封装格式和传输协议。业务数据互联是在公共网络环境下实现分布式网络安全试验平台业务互联的基础。

### 5.3.4 资源控制层

为实现网络安全试验平台之间的资源共享、集成和互操作，目标网络构建方在构建复杂目标网络时，需要对位于不同网络安全试验平台的资源进行编程和调度，为此，需要定义统一的资源配置管理接口。资源控制层提供资源配置管理接口的定义和描述。资源控制互联是实现分布式网络统一调度的基础能力。

网络安全试验平台中的资源，包括：工作站、服务器等计算与存储设备，路由器、交换机等网络设备，入侵检测系统、防火墙等安全防护设备，以及物联网和工业互联网中的专有设备等；也包括镜像、虚拟设备、系统的仿真环境等软件。由于某些网络安全试验平台不具备资源管理功能，因此该层次的互联是非强制的，仅具有相应能力并且愿意提供相应能力的网络安全试验平台进行该层次互联即可。

### 5.3.5 业务管理层

基于网络安全试验平台提供的基础环境和服务，业务管理层根据用户的仿真需求，通过对不同仿真平台的业务仿真功能单元进行组合，以服务实例的形式构建业务仿真试验环境，业务管理互联使得不同网络安全试验平台之间可基于仿真任务描述脚本实现分布式协作，开展多种类型的网络安全相关业务。

## 6 互联互通

### 6.1 基础网络互联

#### 6.1.1 概述

对网络安全试验平台互联过程中，链路层、网络层、传输层等功能进行描述，并针对通信隧道提出容错和负载均衡等管理建议，以及加密和认证等安全性建议，为网络安全试验平台互联提供稳定和安全的底层网络通信。

基础网络互联是实现单点对单点互联的基本能力。

#### 6.1.2 功能

基础网络互联功能如下：

a) 网络互联：基于多种 WAN 链路建立隧道，支持隧道两端的分支机构通过隧道互联互通；
b) 按需组网：根据实验要求动态组网，可基于标准路由协议实现路由控制（BGP、OSPF、ISIS 等）；支持对不同用户构建相互隔离的 VxLAN 封装的 2 层或 3 层叠加 VPN 网络；
c) 数据传输：基于 IP 分组承载高层业务协议，提供网络安全传输协议对 IP 分组提供安全保护（机密性、完整性、可用性）。

d) 可靠性

基础网络互联的可靠性如下：

a) 容错：网络互联具有容错能力，可基于低质量链路实现互联，可基于多条异构链路实现备份互联；
b) Qos：根据业务要求对网络流量进行分类处理，基于 Qos 策略分级处理。

### 6.1.4 安全性

基础网络互联的安全性如下：

a) 内容安全：保证数据传输过程不受基础网络环境影响，不对基础网络环境造成破坏，数据内容不泄露、不可被伪造篡改；
b) 身份可信：基于可信身份实施网络互联。在网络互联以前，需要完成双向鉴权；
c) 边界防护：基于身份认证结果实施网络边界防护和网络访问控制。

## 6.2 业务数据互联

### 6.2.1 概述

业务数据包括开展分布式网络空间安全仿真的试验数据、控制数据和管理数据。业务数据互联对业务数据的组成、属性描述、传输格式、解读方式进行描述，在网络安全试验平台之间实现业务数据的适配、理解和复用。基于业务数据互联，可实现不同网络安全试验平台业务数据的融合与集成。

### 6.2.2 功能

业务数据互联功能描述如下：

a) 业务数据描述：试验数据描述：提供一种试验数据的描述方法，以实现网络安全试验平台之间的试验数据交换；
b) 控制数据描述：提供一种控制数据的描述方法，以支撑网络安全试验平台之间资源调用、试验控制等；
c) 管理数据描述：提供一种管理数据的描述方法，以支撑网络安全试验平台之间应用层数据的交换、协作展开试验等；
d) 数据交换协议：提供一种数据交换协议，以保证网络安全试验平台之间的各类数据可以准确、高效、安全的交换；
e) 互联接口：提供业务数据的封装和解封装的方法，以支撑业务数据在网络安全试验平台之间的传输；
f) 交互模式：提供同步和异步的数据交互模式，提供单播组播等多种通信交互模式，以支撑业务数据在网络安全试验平台之间高效的交换。

g) 安全性

业务数据互联的安全性描述如下：

a) 可验证性：需要提供证明自我真实性的机制；
b) 不可否认性：需要提供数据来源不可否认保护机制；

c) 资源控制互联

6.3.1 概述

对分网络安全试验平台资源进行描述、预约、配置、管理等，提出安全管理的具体建议，支撑分布式试验任务中试验资源的共享利用和场景构建与互联管理，对分布式试验任务场景进行管理，能够适配不同类型的网络安全试验平台系统和不同的应用场景，从而实现各网络安全试验平台资源的互联互通。

6.3.2 功能

资源控制互联功能描述如下：

a) 资源描述：提供一种资源描述方法，使得不同网络安全试验平台在资源互联互通过程中，可以采用统一的资源描述；
b) 资源注册：提供一种资源注册服务，使得一个网络安全试验平台可通知其他网络安全试验平台其可供访问的资源；
c) 资源预约：提供一种资源预约服务，在一个网络安全试验平台访问其他网络安全试验平台资源之前，可以先进行预约，确认资源的可用性；
d) 资源配置：提供一种资源配置服务，在一个网络安全试验平台访问其他网络安全试验平台资源之前，可以对该资源进行配置，以更灵活的使用其他网络安全试验平台资源；
e) 资源管理：提供一种资源管理服务，使得一个网络安全试验平台可以查看、添加、修改、更新其他网络安全试验平台注册的资源。

f) 管理功能

资源控制互联的管理功能描述如下：

a) 配置管理：对资源进行配置管理；
b) 故障管理：对资源进行故障分析和诊断；
c) 性能管理：获取资源的性能和状态；
d) 审计管理：对资源使用情况数据进行采集。

e) 安全性

资源控制互联的安全性描述如下：

a) 身份认证：宜提供一种身份认证服务，认证使用人员的身份；
b) 访问控制：宜提供一种访问控制机制，使得资源在指定的方式下被访问和控制等。

c) 业务管理互联

6.4.1 概述

业务是对分布式网络空间安全仿真行为的统称。业务管理对业务开展过程进行设计与控制。业务描述是对业务过程的任务级描述。业务管理互联在异构网络安全试验平台之间实现业务的协同开展。

### 6.4.2 功能

业务管理互联的功能描述如下：

a) 试验任务描述：对试验任务过程及相关信息进行描述，两个或多个网络安全试验平台开展联合试验之前，先规划好时间、地点、人员、资源使用情况、试验内容等，保证试验任务描述可理解；

b) 试验任务调度：提供试验调度的能力，在两个或多个网络安全试验平台进行联合试验，可以统一控制时间的开始、暂停、恢复、停止、故障排查、回放等；

c) 数据采集：提供数据采集能力，两个或多个网络安全试验平台进行联合试验时，在支持的网络安全试验平台进行指定的数据采集；

d) 数据标识：为每个独立试验提供独立的数据标识；

e) 数据解析：提供数据解析能力，在两个或多个网络安全试验平台进行联合试验时，对采集到的数据，进行统一的计算、分析、展示等；

f) 数据存储：提供数据存储能力，将两个或多个网络安全试验平台的联合试验数据进行统一划分和存储等。

### g) 安全性

业务管理互联的安全性描述如下：

a) 试验隔离：提供试验隔离机制，隔离不同试验的试验环境、数据等；

b) 行为审计：提供至少一种行为审计服务，对网络安全试验平台用户的使用行为进行审计。

# 附 录 A
（资料性）
## 通过互联四个层次协同完成试验的示例

步骤 1.基础网络互联：两个异地的网络安全试验平台，具备互联网出口，同时部署互联网关设备，

通过互联网，网关设备实现互通，同时实现远程的网关设备管理配置能力。

步骤 2.业务数据互联：在网关设备之间建立 wireguard 加密隧道，实现业务数据的加密，在加密隧道上通过 vxlan 协议实现靶标资源的互通。

步骤 3.资源控制互联：两个网络安全试验平台的虚机，防火墙，靶标等资源通过 vxlan 具备远程互通能力及灵活构建虚拟网络能力后，通过资源控制，根据试验场景需要数量的资源，将资源构建到同一虚拟网络中，实现资源的互通。

步骤 4.业务管理互联：资源互通后，通过业务管理启动两个异地的网络安全试验，同时可以开启试验中各种数据的采集分析存储等

步骤 5.试验结束后，业务管理层驱动资源控制层，释放试验资源，然后资源控制层驱动业务数据层删除 vxlan 通道，切断资源之间的互通能力，基础网络根据双方的需求确定是否保持常态化连接。

# 附 录 B
（资料性）
异构靶场互联参考

无人机和卫星等依赖中转设备的，中转设备包含在试验平台中,中转设备通过互联网连接到其它试验平台，如图 B.1 所示，无人机通过基站接入互联网，基站做为中转设备，包含在网络安全试验平台中。

电力网络等与互联网隔离的异构靶场，试验时通过 5G CPE 临时与其它试验平台通过互联网互联，如图 B.1 所示，试验结束后断开。

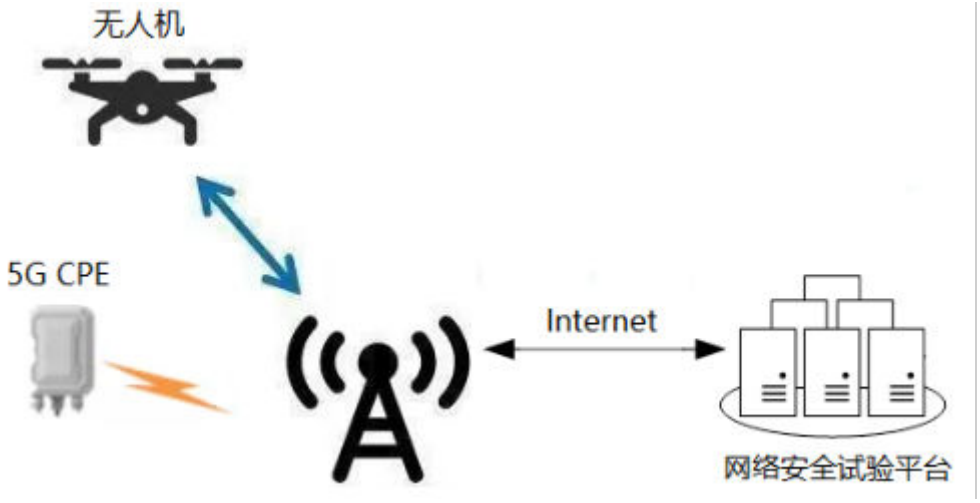



图 B.1 试验平台与无人机和无互联网出口的电力等靶场互联

# 参 考 文 献

[1] GB/T 20986—2023《信息安全技术 网络安全事件分类分级指南》
[2] YD/T 4588—2023《网络空间安全仿真 参考架构》
[3] YD/T 4593—2023《网络空间安全仿真 平台试验操作要求》
[4] YD/T 6007-2024《分布式网络空间安全仿真 互联总体要求》
[5] YD/T 7253-2026《分布式网络空间安全仿真 基础网络互联技术要求》
[6] YD/T 7256-2026《分布式网络空间安全仿真 业务数据互联技术要求》
[7] YD/T 7255-2026《分布式网络空间安全仿真 资源控制互联技术要求》
[8] YD/T 7254-2026《分布式网络空间安全仿真 业务管理互联技术要求》