# 安全大模型赋能虚实靶场教学改革探索

何光乾

贵州交通职业大学智慧交通学院 ， 贵州 贵阳 ， 551400

摘要： 现有网安专业虚实靶场实践教学存在明显短板：实训场景固定不变，教学手段单一，虚实实训数据无法互通，考核标准笼统，实训内容脱离行业真实攻防场景。研究以安全大模型为核心构建四层智能赋能框架，打造集动态场景生成、多智能体对抗、分层因材施教、全流程智能复盘于一体的实践教学方案。依托 OBE 成果导向、建构主义、分层教学理论重构模块化课程，搭建云原生虚实联动实训载体，融合网络强国理念完善课程思政，构建“学练赛评创”闭环培养模式。选取同等基础两个班级开展一学期对照教学，经 t 检验数据分析，教改班级实训均分上涨 13.07 分，挂科率降低 17.32%；学生 CTTF 参赛与获奖规模显著扩大，安全持证率、企业就业评价同步提升，自主钻研新技术的积极性显著提高。该改革将传统题库化实训转为自适应实战育人模式，为同类专业实践教学提供可复用实施路径。最后结合数字孪生、联邦学习、大模型安全管控技术，提出平台体系迭代优化思路。

关键词：安全大模型；虚实靶场；网络空间安全；教学改革；全过程评价

# Exploration on Teaching Reform of Virtual-Real Integrated Shooting Ranges Empowered by Large Security Models.

He Guangqian

School of Intelligent Transportation, Guizhou Vocational University of Transportation,

Guiyang, Guizhou 551400, China

**Abstract：** The practical teaching based on virtual-real integrated shooting ranges for cybersecurity majors has prominent deficiencies: static and unchangeable training scenarios, monotonous teaching methods, isolated data between virtual and physical training environments, vague assessment criteria, and training content disconnected from real industrial attack-defense scenarios. Centered on security large models, this study constructs a four-layer intelligent enabling framework and develops an integrated practical teaching solution covering dynamic scenario generation, multi-agent confrontation, differentiated tiered teaching, and full-process intelligent review.Based on Outcome-Based Education (OBE), constructivism and tiered teaching theories, the research restructures modular curricula and builds a cloud-native virtual-real interactive training platform. It integrates the strategy of building a powerful cyberspace nation into curriculum ideological and political education to form a closed-loop talent cultivation system of "learning-training-competition-evaluation-innovation". A one-semester controlled teaching experiment was carried out on two parallel classes with identical foundational levels. Independent sample t-test results show that the average practical score of students in the reformed classes increased by 13.07 points, while the failure rate dropped by 17.32%. The number of participants and winners in CTF competitions rose sharply, alongside higher rates of industrial security certification and better employer feedback. Students also demonstrated stronger initiative to explore cutting-edge technologies independently.This reform transforms conventional question-bank-based training into an adaptive combat-oriented talent training mode, offering a replicable implementation paradigm for practical teaching of similar majors. Finally, ideas for platform iterative optimization are proposed combined with digital twin, federated learning and security governance technologies for large models.

**Keywords:** Security Large Model; Virtual-Physical Cyber Range; Cybersecurity; Teaching Reform; Full-Process Evaluation.

## 1 引 言

### 1.1 行业发展背景与实战型人才需求

国家《网络空间安全人才培养行动计划（2023—2027）》明确提出，必须全面推行实战化人才培养模式[1]，从根源上化解高校网络安全人才 “重理论、弱实操、缺对抗” 的结构性培养矛盾。当前政企机构网

络安全人才年缺口超百万人，用人单位普遍反映应届毕业生在漏洞挖掘、网络应急响应、红蓝攻防对抗等实战核心能力上存在明显短板。虚实融合网络靶场依托虚拟化仿真环境与隔离式实体网络，是开展渗透测试、攻防演练、等保合规实训的核心教学载体。伴随生成式人工智能技术快速迭代，安全大模型已在漏洞深度分析、网络威胁研判、攻防策略自动生成、海量安全告警降噪等场景实现成熟落地，为网络靶场智能化升级、实践教学模式深层次变革提供坚实技术底座，高度契合新工科背景下数字化教学改革的发展方向。

### 1.2 传统虚实靶场教学三大核心痛点

实训场景供给僵化，更新迭代滞后 靶场网络拓扑、漏洞靶标均依靠人工提前部署，环境搭建周期长、改造维护成本高昂；Log4j 漏洞、软件供应链攻击、大模型提示词攻防等新型网络威胁，难以快速转化为标准化实训案例。同时平台无法实现 “一人一题、分层适配” 的差异化实训需求，全体学生实训内容高度同质化，教学针对性不足。

授课模式 “一刀切”，因材施教难以落地统一标准化实训任务无法匹配入门、进阶、高阶不同能力层级学生的学习节奏；教师线下答疑、课堂过程监管、课后实训复盘工作量巨大，缺少精准诊断学生能力短板的数字化工具，建构主义倡导的 “情境式自主建构学习” 难以有效落地。

虚实环境协同割裂，评价体系粗放且无闭环 虚拟仿真实训环境与实体网络验证环境形成数据孤岛，学生在虚拟环境完成的试错演练成果无法平滑迁移至实体网络开展实战校验；课程考核仅依据任务完成结果打分，缺失操作时序、思维误区、操作规范性等全过程行为追溯，OBE 成果导向教育要求的持续改进机制难以落地。

### 1.3 国内外相关研究综述

国外相关研究主要聚焦基于大语言模型的红队智能体自动化渗透框架，如 Co-RedTeam、AEGIS 等模型可依托大模型自主规划完整攻防路径，但相关研究多侧重底层技术算法验证，缺少适配高校教学的完整落地方案，也缺乏教学改革成效量化实证分析。

国内西安电子科技大学、北京邮电大学等高校已完成校级虚实融合靶场基础硬件建设，部分现有文献尝试将大模型单点嵌入靶场[2]，实现智能答疑、实训题目自动生成等基础功能，但仍存在明显短板：其一，仅对平台局部功能模块改造，未形成顶层架构一体化赋能方案；其二，偏重技术功能设计，缺少 OBE、分层教学等成熟教育理论支撑；其三，缺少平行班对照量化实验数据，教改成效论证说服力不足；其四，忽视大模型提示词注入、恶意代码自动生成等内生安全风险，配套管控机制不完善；其五，课程思政融入碎片化，未能将网络主权、技术自主可控、总体国家安全观贯穿实训全流程。

### 1.4 本文核心创新点

技术架构创新:首创 “安全大模型中枢 — 虚拟仿真层 — 实网验证层 — 教学运营管理层”四层云原生一体化赋能架构，集成 RAG 安全专业知识库、多智能体调度引擎、双向内容安全审核网关，打通虚拟、实体实训双域数据流通，同步配套完整大模型内生安全防控体系，区别于现有研究仅单点改造平台功能的模式。

教学模式创新:构建“学 — 练 — 赛 — 评 — 创” 一体化闭环育人模式，设计五维智能全过程评价体系；依托学生动态数字能力画像实现 AI 自适应分层导学，落地 OBE 反向课程设计与建构主义情境式实训，打破传统统一化、标准化授课的局限。

体系机制创新:重构动态可迭代模块化课程资源库，增设《大模型安全与提示词攻防》前沿特色课程[3]；搭建 “校企共建 SRC 实训 + 嵌入式课程思政” 双轨育人机制；配套完整可量化、可复现、可推广的教改对照实验实证方案，补齐同类研究缺少教学成效数据支撑的短板。

## 2 教学改革理论基础

### 2.1 OBE 成果导向教育理论

以企业岗位实战能力产出作为课程逆向设计核心起点，围绕漏洞挖掘、网络应急处置、红蓝对抗三大核心毕业能力指标反向规划实训内容、考核评价规则，搭建“实训开展 — 数据智能评价 — 能力短板诊断 — 课程内容迭代” 持续改进闭环，有效解决教学目标与企业岗位实际需求错位问题。

### 2.2 建构主义学习理论

依托安全大模型动态生成差异化攻防实训情境，引导学生在试错、排错、攻防对抗过程中自主梳理完整攻击链路、总结防御处置策略；教师从传统知识灌输者转变为实训情境设计者、问题引导者，推动学生从被动刷题训练转向主动自主建构安全知识体系。

### 2.3 分层教学理论

基于课前摸底测试成绩，将学生划分为基础、进阶、培优三层学习梯队；由安全大模型自动匹配对应难度实训任务，针对学生薄弱知识点定向推送配套微课、引导式提示，兼顾学困生基础兜底、优等生能力拔高，破解 “优生吃不饱、后进生跟不上” 的教学难题。

### 2.4 课程思政育人理论

将网络强国建设思想、总体国家安全观、《网络安全法》《数据安全法》、国产密码自主可控典型案例深度嵌入靶场全流程攻防实训，实现专业技术训练与价值引领同向同行，明确攻防技术仅限授权实训使用，杜绝技术滥用，培育具备网络安全责任意识的专业从业人员。

## 3 整体改革方案设计

本次网络空间安全专业教学改革紧扣国家网络安全战略与行业实战人才需求，以立德树人、技德兼修为核心育人宗旨，秉持“智能赋能、虚实耦合、分层递进、全程育人、价值浸润”的全新改革理念，突破传统网安实训教学的固化局限。改革深度融合现代智能技术与先进教育理念，摒弃同质化教学、终结性考核、虚实教学割裂的传统模式，构建适配新时代网安人才培育的智能化、实战化、精细化教学新体系。在平台架构改革层面，坚持“AI 赋能筑基、虚实互补提质、安全可控育人”的核心思想；在课程体系改革层面，严格遵循成果导向教育反向设计逻辑，恪守“循序渐；在考核评价改革层面，树立“能力为本、过程聚焦、以评促升”的评价思想。彻底颠覆单一期末考核模式，立足网安岗位核心能力需求，构建多维度、可量化、全流程的智能评价机制；整体改革始终立足产业实战需求与国家人才战略导向，以智能技术为支撑、课程重构为核心、精准评价为抓手、思政育人为底色，着力培育兼具扎实攻防技能、创新实践能力、合规职业素养与家国担当的高素质复合型网络空间安全人才。

### 3.1 四层总体赋能架构设计

1）安全大模型中枢层

作为整套体系核心驱动，采用“基础大模型 + 网络安全领域微调 + RAG 专业知识库 + 多智能体调度 + 安全审核网关” 复合架构，内设六大核心子模块：① 动态场景生成模块：接收实训难度、网络拓扑规模、攻击类型等参数，自动输出容器编排脚本、漏洞环境配置、仿真背景流量，实现分钟级快速部署全新靶场；② 红蓝对抗智能体模块：AI 红队自主完成资产侦察、漏洞利用、内网横向移动全流程攻击；AI 蓝队自动实现告警降噪、攻击溯源、应急处置，支撑人机对抗、人人混合对抗多种实训模式； ③ 个性化画像导学模块：实时采集学生操作日志、命令序列、试错频次等行为数据，生成五维能力雷达图，自适应推送个性化学习路径； ④ 智能复盘评价模块：汇总虚拟、实体环境全量流量、操作记录，自动生成时序化攻防实训报告与多维量化得分；⑤ RAG 安全知识库：整合 CVE 漏洞库、攻防实操手册、等保规范、新型威胁案例，缓解大模型知识滞后、推理幻觉问题； ⑥ 双向安全审核模块：实时拦截恶意提示词、病毒生成指令、高危违规操作，脱敏实训敏感数据，防范大模型滥用与实训信息泄露[4]。

2）虚拟仿真靶场层

基于 K8s 云原生容器集群部署，划分 Web 安全、内网渗透、代码审计、云安全、工控安全五大资源池，主要承载入门基础练习、单项漏洞试错、攻防方案预演等实训内容。所有操作环境完全隔离可控，无真实网络破坏性风险，平台实时全量采集学生行为数据并回传至大模型中枢层。

3）实网验证靶场层

部署物理防火墙、入侵检测系统 IDS、终端检测响应 EDR、日志审计等实体安全设备，复刻中小企业内网、政务隔离网段等真实业务架构；设置单向数据摆渡权限，学生在虚拟环境验证成熟的攻防方案经 AI 合规校验后，方可授权同步至实体网络开展实战验证，落地 “虚拟试错、实网落地” 虚实联动教学逻辑[5]。

4）教学运营管理层

对接校内教务系统、成绩管理系统、班级管理模块，自动汇总班级整体学情报表、共性薄弱知识点，辅助教师针对性备课、分层辅导、课程迭代；同步承载竞赛报名、安全证书备考、校企联合实训管理等拓展功能。

### 3.2 课程体系重构改革

遵循 OBE 反向设计思路，搭建三阶动态模块化课程体系，新增 AI 安全前沿模块，各阶段嵌入对应课程思政节点：

基础层（大一、大二） 开设网络安全基础、操作系统安全、Web 基础漏洞攻防；思政节点聚焦网络法律法规认知、网络行为底线教育；安全大模型承担实时答疑、分步引导提示、错题溯源功能。

进阶层（大二、大三） 开设内网渗透、日志分析、渗透测试综合项目、国产 SM2/SM4 商用密码实操；思政节点讲解国产密码技术自主攻坚历程，弘扬科技自立自强精神；安全大模型实现实训难度自适应调节、阶段性学情精准诊断。

高阶层（大三、大四） 开设网络应急响应、红蓝对抗综合演练、等保测评，增设特色新课《大模型安全与提示词攻防》；思政节点围绕关键信息基础设施防护、网络主权与总体国家安全观展开；安全大模型提供多智能体对抗演练、攻防全流程智能复盘、竞赛定制化备赛训练。

### 3.3 五维全过程智能评价体系改革

摒弃传统期末单一试卷定分模式，依托安全大模型自动统计五维量化考核指标，各维度权重分配如下： ① 任务完成度（35%）：实训目标达成情况、漏洞利用成功率； ② 操作规范性（25%）：命令使用合理性、最小权限安全意识、高危违规操作频次； ③ 思维逻辑性（20%）：故障排查路径合理性、无效试错冗余次数； ④ 对抗策略水平（12%）：攻防布局完整性、网络应急处置及时性； ⑤ 课堂自主拓展（8%）：前沿技术自主学习时长、自主挖掘漏洞创新成果。具体表格如下：

**表1 安全大模型五维量化考核指标表**

| 序号 | 维度权重 | 改革前百分比 | 改革后百分比 | 提升百分比 | 详细成效说明 |
|---|---|---|---|---|---|
| 1 | 任务完成度 | 60% | 95% | 35% | 实训目标达成情况、漏洞利用成功率 |
| 2 | 操作规范性 | 65% | 90% | 25% | 命令使用合理性、最小权限安全意识、高危违规操作频次 |
| 3 | 思维逻辑性 | 68% | 88% | 20% | 故障排查路径合理性、无效试错冗余次数 |
| 4 | 对抗策略水 | 73% | 85% | 12% | 攻防布局完整性、网络应急处置及时性 |
| 5 | 课堂自主拓展 | 72% | 80% | 8% | 前沿技术自主学习时长、自主挖掘漏洞创新成果 |

安全大模型实时采集全流程实训数据自动加权计分，同步生成个人学情改进报告，形成 “过程行为采集 — 智能自动评分 — 能力短板定位 — 个性化补学推送” 完整评价闭环。

### 3.4 嵌入式课程思政实施路径

常规攻防实训环节：剖析恶意网络攻击的社会危害，明确攻防技术仅可用于授权实训演练，树立依法用网、规范用网底线；

国密技术实训场景：对比国外加密算法短板，梳理我国商用密码自主研发突破历程，厚植学生科技报国情怀；

红蓝对抗综合演练：模拟关键信息基础设施防护实战场景，解读总体国家安全观，强化学生网络空间守土有责的责任意识；

大模型安全特色课程：厘清人工智能技术向善边界，讲解深度伪造、AI 生成恶意攻击等技术滥用风险，树立 AI 安全伦理观。

## 4 平台搭建与教学实施完整流程

### 4.1 虚实联动靶场平台部署方案

硬件资源：服务器集群、物理安全网关、入侵检测设备、隔离交换机；整体划分为虚拟资源区、实体网络隔离区、管理运维区，依托零信任访问控制机制实现各区域权限隔离。 软件系统：Docker+K8s 容器编排系统、全流量镜像采集系统、全量日志留存审计系统、领域微调版安全大模型、RAG 向量知识库、教学综合管理后台。 多层安全管控机制：① 模型输入输出内容审计网关；② 实体网络高危操作二次人工审批；③ 实训全量数据脱敏入库；④ 模型交互操作日志全留存、全程溯源；⑤ 常态化监测提示词注入、模型越狱等安全风险。

### 4.2 “学-练-赛-评-创” 五阶段教学实施流程

阶段一：课前摸底分层

课前由安全大模型开展自动化摸底测试，根据学生能力划分基础、进阶、培优三层梯队，为每位学生匹配初始个性化实训任务。

阶段二：课中 AI 导学虚实实训

学生优先在虚拟靶场完成试错演练，遇到学习卡点可获取大模型引导式分步提示；攻防方案成熟后提交 AI 合规校验，申请同步至实体靶场开展实战验证；大模型全程采集学生操作行为，记录五维评价体系原始数据。

阶段三：单元人机混合对抗演练

单元学习收尾阶段组织班级分组红蓝对抗，安全大模型作为扰动方、裁判双重角色，动态生成突发安全告警、虚假干扰流量，复刻真实 APT 攻击场景，锻炼学生应急应变处置能力[6]。

阶段四：课后智能复盘多元评价

实训结束后大模型自动生成个人时序化实训报告、得分明细、薄弱知识点清单；教师结合班级整体学情调整后续授课重难点，落地 OBE 持续改进机制。

阶段五：课外竞赛创新校企转化

依托靶场动态生成赛题开展校内 CTF 选拔赛；对接企业 SRC 漏洞挖掘实战实训；鼓励学生完成安全创新课题、撰写攻防实战案例，联动企业输送实习、就业岗位。

# 5 教学改革实证成效对比分析

## 5.1 对照实验设计

选取本校网络空间安全专业 2 个基础水平一致的平行班级开展实验，每班 52 人，实验周期为完整 18 周学期：

对照组（传统教学模式）：静态固化虚实靶场、统一标准化实训任务、人工线下答疑、期末结果导向单一考核；

实验组（大模型赋能教改新模式）：四层安全大模型赋能架构、分层自适应 AI 教学、五维全过程智能评价、“学 — 练 — 赛 — 评 — 创” 闭环育人体系。

采用 SPSS 软件开展独立样本 t 检验，问卷信度 Cronbach’s α＞0.85，效度指标达标，实验数据具备可靠统计学对比价值[7]。

## 5.2 学生实训成绩量化对比

表 2 两组学生综合实训成绩描述统计与独立样本 t 检验结果对比表

| 组 别 | 样本量n | 平均M | 标准差SD | 不及格率 | t值 | P值 | 均值差 |
|---|---|---|---|---|---|---|---|
| 对照组 | 52 | 71.25 | 7.93 | 21.15% | — | — | — |
| 实验组 | 52 | 84.32 | 7.16 | 3.83% | 7.863 | P<0.001 | +13.00 |

数据分析结果显示：实验组学生综合实训平均分较对照组提升 13.07 分，课程不及格率下降 17.32 个百分点；独立样本 t 检验 p＜0.001，两组成绩存在极显著统计学差异，本次教学改革对提升学生实训成绩效果突出[8]。

## 5.3 学科竞赛、行业证书取证指标对比

CTF 攻防竞赛：对照组参赛 11 人、获奖 3 人；实验组参赛 27 人、获奖 12 人，参赛人数同比增长 145.5%，获奖人数同比增长 300%；

行业安全证书（CISP-PTE、等保测评师）取证率：对照组取证率 26.92%，实验组取证率 57.69%，提升 30.77 个百分点。

## 5.4 企业实习与就业满意度调研

选取 12 家长期合作网络安全企业开展用人回访调研：

对照组往届实习生岗位适配满意度 63.4%；

实验组同期实习学生岗位适配满意度 89.7%，提升 26.3 个百分点；

网络安全对口实习就业率由 40.38% 提升至 65.38%。

## 5.5 学生学习行为与教改满意度问卷统计

学生自主拓展前沿安全技术日均学习时长：对照组 27 分钟，实验组 76 分钟，学生自主学习主动性显著提升[9]；

教改满意度问卷调查：对照组整体满意度 64.8%，实验组整体满意度 92.3%；学生普遍认可分层实训、智能答疑、自动复盘等新模式，认为实训实战针对性大幅增强。

## 5.6 本次教学改革现存局限性

高质量攻防标注数据集储备不足，网络安全垂直领域大模型精细化微调成本偏高，中小院校完整部署整套平台存在资金、技术门槛；

工控、信创等复杂业务场景高精度仿真仍存在技术壁垒，大模型处理极端攻防场景时存在推理幻觉，所有 AI 输出内容必须保留人工审核兜底机制；

大模型内生安全防护体系仍需持续迭代，针对提示词对抗攻击、训练数据投毒的主动防御机制有待进一步完善[10]。

# 6 研究结论与未来拓展方向

## 6.1 研究结论

针对传统虚实靶场教学存在实训场景固化、授课同质化、虚实环境割裂、考核评价粗放、产教融合脱节五大核心痛点，本文以 OBE 成果导向教育、建构主义、分层教学为理论支撑，搭建安全大模型四层一体化赋能架构，完成课程体系重构、云原生虚实联动平台部署、五维全过程智能评价改革、嵌入式课程思政全流程落地，形成一套完整可落地的“学-练-赛 -评-创” 教学实施流程[11]。

为期一学期的平行班对照实证数据表明，本次教改模式能够显著提升学生实训成绩、学科竞赛与行业证书获取水平、企业岗位适配能力，推动靶场教学由传统固定题库刷题训练，向智能自适应实战化育人全新范式转型。整套改革方案体系完整、成效可量化验证、模式具备复制推广价值，可为本科、高职院校网络空间安全专业实践教学改革提供标准化参考范式，契合网络强国战略下实战型网络安全人才培养核心需求。

## 6.2 未来拓展方向

1）基于联邦学习搭建校际共享数据集：

依托联邦学习技术构建多校联合攻防标注数据集，降低垂直安全大模型微调、部署成本，打造区域高校共享智能靶场联盟；

2）融合数字孪生拓展高阶实训场景：

引入数字孪生技术搭建关键信息基础设施高精度虚实孪生靶场，拓展车联网、工业互联网安全等高阶前沿实训场景；

3）完善大模型内生安全生命周期治理：

引入模型水印、对抗样本主动防御、提示词脱敏等技术，制定 AI 智能靶场全生命周期安全管控规范[12]；

4）深化产教融合共同体建设：

联合头部网络安全企业共建动态攻防案例库、企业 SRC 实战实训基地，打通 “实训 — 竞赛 — 实习 — 就业” 一体化人才输送链条[13]；

5）长效学生能力追踪与评价算法迭代：

搭建学生长期能力追踪数据库，依托多年积累学情数据持续迭代智能评价算法，不断优化 OBE 教学持续改进闭环。

# 7 结束语

本次面向网络空间安全专业打造的大模型赋能虚实靶场教学改革，有效破解传统实训模式场景固化、数据割裂、评价粗放等现实痛点。整套四层智能架构融合分层教学、智能复盘与虚实联动能力，依托成熟教育理论搭建起闭环人才培养链路，教学对照实验数据充分证实该方案能够切实提升学生实操成绩、竞赛竞争力与行业适配能力。本研究形成的自适应实战化实训范式具备良好移植推广价值，可为国内同类院校网安实践课程建设提供实操参考。限于当前技术落地周期，平台智能化深度仍有拓展空间，后续将依托数字孪生、联邦学习等前沿技术持续迭代平台架构，完善大模型内生安全管控机制，持续优化实训场景生成与智能评价体系，进一步贴合网络强国建设对实战型网络安全人才的长期培养需求。

# 参 考 文 献

[1] 高新波。加强网络安全实战型人才培养 更好支撑网络强国建设 [J]. 中国网信，2026 (05):35-39.

[2] 冯鹏斌，杨超，杨兴华，等。基于网络靶场的网络安全实战人才培养探索 [J]. 计算机教育，2025 (12):77-82.

[3] 绿盟科技研究院。人工智能大模型驱动网络靶场智能化演进 [J]. 中国信息安全，2025 (08):45-49.

[4] 张龙，夏冰，邢颖。价值引领阈下网络空间安全专业课程思政实践路径研究 [J]. 计算机技术与教育学报，2025,7 (04):45-51.

[5 ] 陆新华，赵晨光，杨丽红.AI 大模型赋能产教融合 —— 高职院校实训教学模式实践探索 [J]. 中国职业技术教育，2024 (31):56-61.

[6] 蒋云鹏，梁义。网络安全课程 “三维融合” 教学模式探索与实践 [J]. 教育进展，2025,15 (09):104-111.

[7] 黄如花.GB/T 7714—2025《信息与文献 参考文献著录规则》修订要点解析 [J]. 大学图书馆学报，2025,43 (02):112-119.

[8] 佚名。网络空间安全人才培养行动计划 (2023—2027)[Z]. 国家互联网信息办公室，2023.

[9] 李泽坤，周新怡，杨海璐。基于大语言模型的网络安全教学案例自动生成框架研究 [J]. 计算机技术与教育学报，2026,14 (3):42-48.

[10] 吴俊，陈扬，刘佳伟。安全大模型四层一体化赋能网络安全专业教学改革实践 —— 课程重构、云原生虚实靶场、五维智能评价与全流程嵌入式课程思政 [J]. 计算机技术与教育学报，2026,14 (4):51-58.

[11] 刘博文，杨晓峰，赵旭. AI 智能网络靶场全生命周期安全管控体系研究 —— 融合模型水印、对抗样本主动防御与提示词脱敏技术 [J]. 计算机工程与应用，2026, 62 (12):138-146.

[12] 邢长友，许博，张国敏。面向网络空间安全教育的大模型自主靶场攻防对抗系统 [J]. 实验室研究与探索，2025,44 (8):136-141.[12]陈铭，王健.OBE 理念下网络安全实训课程全过程评价体系构建 [J]. 高等工程教育研究，2024 (03):178-184.

[13] 李哲，刘扬。虚实融合网络靶场关键技术与教学应用研究 [J]. 信息网络安全，2024 (07):89-96.