面向网络安全系列课程的“产教融合、赛课融通”教学改革探索*

卢晓珍[1**] 陈兵[1] 肖亮[2] 胡峰[1]

1.南京航空航天大学计算机科学与技术学院，南京 211106 2.厦门大学 信息学院，厦门 361005

摘 要 针对网络安全系列课程教学中存在的理论与实践脱节、攻防能力培养薄弱等问题，分析传统教学方式在培养应用型人才方面的局限性，提出“产教融合、赛课融通”的网络安全系列课程教学改革观点。以前沿技术为牵引、以实战能力为导向，整合产业实践资源，将科创训练、学科竞赛与项目式实习系统嵌入教学全过程，构建全链路网络安全人才培养框架，促进学生知识、能力与素质的协同发展，为网络安全人才培养提供可复用的实践路径。

关键词 网络安全，教学改革，产教融合，赛课融通

Exploration of Teaching Reform for Cybersecurity Course Series Based on Industry-Education Integration and Competition-Course Combination*

Xiaozhen Lu[1] Bing Chen[1] Liang Xiao[2] Feng Hu[1]

1. School of Computer Science and Technology Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China

2.School of Information Xiamen University, Xiamen 361005, China

Abstract—To address the prominent issues of disconnection between theory and practice, as well as the weak cultivation of offensive and defensive capabilities in cybersecurity course series teaching, this paper systematically analyzes the structural limitations of traditional teaching models in cultivating application-oriented talents, and proposes a reform paradigm of industry-education integration and competition-course combination for cybersecurity course series. Guided by cutting-edge technologies and oriented toward practical combat capabilities, this paradigm deeply integrates authentic industrial project resources, and organically embeds scientific research innovation training, disciplinary competitions, and project-based internships into the entire teaching cycle. It constructs a full-link talent cultivation framework to promote the collaborative evolution of students' knowledge construction, capability generation, and quality development. This paper provides a reusable practical pathway for cultivating cybersecurity talents.

Keywords—cybersecurity, teaching reform, industry-education integration, competition-course combination

1 引 言

在新一轮科技革命与产业变革纵深推进的背景下，网络空间已成为大国博弈的核心战场，网络安全上升为国家安全的重要组成部分[1-2]。随着人工智能、云计算、物联网等新一代信息基础设施加速融合，网络攻击手段呈现智能化、自动化、隐蔽化趋势，关键信息基础设施面临的 APT 攻击、供应链投毒、AI 驱动型渗透等新型威胁日益严峻，对网络安全防御体系的实时性、精准性和协同性提出了前所未有的挑战[3]。据教育部数据显示，到 2027 年，我国网络安全人员缺口将达 327 万，且随着数字化进程加速，这一缺口将持续扩大，高层次应用型人才供给不足已成为制约我国网络强国战略实施落地的关键瓶颈。

面对日益复杂的网络威胁态势，现有网络安全系列课程教学却存在明显的滞后性[4]：内容滞后于威胁演进，教材更新周期长，对 AI 驱动攻击、云原生攻防等前沿威胁覆盖不足，难以匹配快速迭代的攻防技术生态；方法滞后于技术变革，传统“理论讲授+验证实验”的线性模式难以支撑真实对抗场景下的能力训练，学生缺乏在动态网络环境中进行应急响应的实战思维；能力滞后于行业需求，考核偏重知识记忆，学生缺乏复杂工程问题解决与攻防实战能力。上述三重难题相互交织，暴露出以知识传授为主的传统教学范式在培养应用型网络安全人才方面的深层局限。

*基金资助：国家自然科学基金面上项目“面向低空智能网联的高可靠无线安全通信方法研究”(62571240)。

**通讯作者：卢晓珍 luxiaozhen@nuaa.edu.cn。

针对上述问题，结合国家网络强国战略与新工科建设要求，亟需对网络安全系列课程进行系统性教学改革。“产教融合”整合产业实践资源，将真实项目需求与行业前沿技术引入课堂，打破理论与实践壁垒，驱动知识向能力转化；“赛课融通”依托学科竞赛的高阶对抗压力，激发学生内生动力与创新潜能[5-7]。同时，将智能技术嵌入教学全链路，通过科创训练实现内容动态更新与个性化训练，培养学生新型安全素养。此外，将总体国家安全观、网络强国使命等思政元素融入攻防训练全过程，引导学生树立正确的技术价值观与法律边界意识。

本文基于南京航空航天大学国家级一流本科课程《网络安全》等教学实践，提出“产教融合、赛课融通”的网络安全系列课程教学改革观点，构建融合网络安全基础理论、前沿攻防技术与课程思政要素的教学框架，在强化基础理论的同时引入云原生安全研发与运维、代码安全审计与访问控制、隐私计算与分布式数据安全等工程项目实践，引导学生开展全链路安全系统设计与攻防对抗，并通过科创训练与学科竞赛提升复杂工程问题解决能力，实现专业能力培养与价值引领协同发展，为培养服务网络强国战略的高层次应用型网络安全人才提供可复用的理论与实践参考。

2 传统教学现存问题与局限性

网络安全学科具有鲜明的对抗性、实践性与时效性，攻防技术与安全威胁迭代迅速，对人才实战能力与动态适配能力提出了极高要求。相较行业高速发展态势，传统教学模式体系固化、更新滞后，难以支撑应用型人才培养目标。

2．1 理实体系割裂，教学内容迭代滞后

网络安全领域攻防技术迭代迅速，而传统课程教材内容更新周期长，教学内容多围绕传统网络安全漏洞与经典攻击方式展开，对云安全、人工智能安全等前沿领域内容覆盖不足，对 APT 攻击等新型安全威胁讲解匮乏，导致学生所学知识滞后于实际发展需求。同时，传统网络安全教学采用“理论先行、实验后置”的分段式教学模式，理论课堂侧重讲解网络协议、加密算法、安全机制等抽象理论知识，内容枯燥且偏向书本化；配套实验多为验证性基础实验，仅围绕单一知识点开展简单操作，实验场景固定、流程固化。理论知识与实操训练相互割裂，学生无法将理论与实操对应结合，难以形成完整的知识应用体系。

2．2 实战场景缺失，攻防能力培养薄弱

随着生成式人工智能与自动化攻击技术的普及，网络威胁已呈现显著的智能化特征：攻击者利用 AI 进行漏洞自动挖掘、钓鱼内容生成及渗透路径动态优化，防御侧也普遍部署了基于机器学习的入侵检测、行为分析与自适应防护系统。然而，现有课程教学实验环境多为静态简易模拟环境，网络拓扑结构简单、安全防护层级单一且预设了固定的攻击路径与已知漏洞入口，导致课堂训练与真实业务网络、高水平竞赛实战环境存在结构性差距。在此训练场景下，学生缺乏面对动态威胁的战术博弈与应急处置经验，难以培养攻防思维与实战素养。

2．3 评价体系单一，忽视综合能力考核

现有网络安全系列课程考核仍以期末笔试为主，侧重知识记忆与概念辨析，题型多为选择题、简答题等标准化试题，缺乏对漏洞挖掘、渗透测试、应急响应等实战能力的有效评估。考核过程忽视团队协作、工程实践、创新思维与复杂工程问题解决等综合素质的测评，难以真实反映学生在动态对抗场景下的综合表现。单一的评价导向导致学生重理论轻实践，缺乏主动探索前沿技术与真实攻防场景的内生动力，与网络安全行业对应用型、创新型人才的综合能力需求形成明显错位。

3 网络安全人才培养框架

如图 1 所示，本文提出“产教融合、赛课融通”的网络安全人才培养框架。以“前沿技术牵引、实战能力导向”为核心理念，通过整合产业实践资源与竞赛高阶对抗场景，重构教学内容、方法与评价体系，形成“基础能力训练—攻防对抗实践—综合实战演练”的全链路培养体系，系统解决理实割裂、场景缺失与评价单一三大痛点。

3．1 产教融合，产业资源教学化重构

通过深度产教融合以及与企业共建实验平台，引入企业成熟的网络安全实践资源并嵌入教学全链路，聚焦网络安全领域协同创新与高层次应用型人才培养[8]。在理论教学层面，校企联合开发特色网络安全系列课程，梳理网络安全等课程的功能定位，设计递进式任务结构，使不同课程围绕同一安全问题形成协同关系。由校内导师系统讲授网络协议、密码学原理、访问控制等基础理论知识，企业导师则依托抗量子密码高效适配与实现、云计算数据共享等产业核心技术主导实验教学，将前沿工程实践转化为课堂内容，使学生在多课程学习中逐步深化理解专业知识，形成完整的问题分析体系与系统认知。此外，定期邀请企业技术专家开展系列专题讲座，帮助学生深入理解产业技术迭代的内在逻辑与工程化落地的核心约束，建立从学术原理到产业实践的系统性思维框架。



图 1 “产教融合、赛课融通”的网络安全人才培养框架

在实践教学层面，将企业真实渗透测试报告、漏洞分析文档、应急响应预案等脱敏后转化为教学案例，覆盖人工智能模型安全、物联网边缘安全、云原生攻防等前沿领域的动态案例库，使学生在课堂中直面企业级真实威胁场景与工程决策逻辑。例如，在讲授身份认证与访问控制技术时，引入企业级零信任安全网关的部署与配置案例并延伸至低空经济场景，以无人机集群通信中的轻量级身份认证协议为切入点，分析机载设备在计算资源受限、通信高实时性约束下的认证机制设计需求，帮助学生理解传统 IT 环境与企业级云环境在信任评估、持续身份校验与动态访问控制策略上的差异，建立前沿理论知识与复杂工程场景的映射关系，从而培养从安全需求分析、方案设计到攻防验证的完整工程思维。

3．2 赛课融通，竞赛场景课程化嵌入

结合全国大学生信息安全竞赛等学科竞赛，将学生参赛与课堂实践教学同步进行，以竞赛赛题为实践项目，将学生参赛成绩纳入课程考核。在常规理论课程中，将竞赛中的密码学挑战、Web 渗透等赛题解构为课外实践模块与科创训练课题，学生组队完成技术调研、文献综述、方案设计与工具开发，以项目答辩与学术报告计入实践学分；在集中式实践教学中，将教学周期对齐竞赛的报名、初赛与决赛全流程，使实践启动、中期检查与结项答辩分别对应竞赛各阶段节点，学生参赛成绩直接转化为课程实践成绩，实现备赛过程与实训过程在时空维度与内容结构上的统一。通过建立制度化考核机制，将学科竞赛成绩与科创成果纳入课程评价体系，以赛题作为实践拓展载体，推动课程教学与竞赛训练双向赋能。

组建由多学科课程教师、产业导师与竞赛优秀选手构成的协同指导团队，打破单一课程师资壁垒，依据竞赛方向与学生兴趣实施精准匹配指导，针对竞赛中的复杂技术问题开展课程协同攻关，例如，面对内核提权与漏洞利用链构造类赛题，信息安全导论课程教师主导内核漏洞挖掘与利用技术解析，网络安全课程教师负责网络层攻击路径审计与防御架构设计，使学生在同一赛题中同步调用多学科知识，建立竞赛技能与课程体系的深度关联，形成竞赛驱动、教学相长的指导生态。基于此，帮助学生建立竞赛经验与工程规范的双向映射关系，从而培养从赛题分析、漏洞挖掘到防御加固的全链路工程思维。

3．3 全链路协同，闭环培养与动态迭代

通过贯通“基础能力训练—攻防对抗实践—综合实战演练”三层递进架构，横向耦合产教融合资源通道与赛课融通竞赛通道，形成纵向衔接、横向联动的人才培养闭环。

在基础能力训练阶段，通过将企业真实渗透测试报告、漏洞分析文档与前沿技术案例转化为分级实验项目，把密码学原理、网络协议机制等理论知识嵌入协议逆向、漏洞复现等实操环节，同步融入总体国家安全观教育，引导学生在技术训练中树立网络强国使命意识与法律边界观念。在攻防对抗实践阶段，通过将全国大学生信息安全竞赛等学科竞赛赛题与动态对抗场景引入长周期项目制教学，使学生在密码学挑战、Web 渗透等任务中经历完整的调研、设计、开发与验证流程，在竞赛压力与团队协作中锤炼战术博弈与应急处置能力，并渗透白帽子伦理规范与负责任披露理念，培育正确的技术价值观。在综合实战演练阶段，通过 APT 攻击链溯源、安全系统全生命周期开发等综合项目，以团队协作形式实施全过程能力考核，企业工程师与竞赛专家参与答辩评审，引入行业视角的第三方评价，同时通过将低空经济基础设施安全等国家战略需求场景融入项目设计，使学生在复杂工程问题解决中深化对关键信息基础设施防护战略意义的认知，实现专业能力、工程素养与价值理念的协同培养。

通过建立闭环机制，依托南京航空航天大学国家级一流本科课程《网络安全》等教学实践平台与企业资源，将云原生安全、人工智能安全等新兴领域技术演进动态反馈至教学方案修订与案例库更新，以竞赛排名、企业认证通过率、实习单位评价等多维数据评估培养成效，反向优化课程模块与实验项目设计，推

动培养体系与产业技术前沿的动态适配，实现人才供给与产业需求的精准对接。

4 教学改革成效

通过实施“产教融合、赛课融通”的网络安全系列课程教学改革，我校在近年的教学实践中取得以下突出成效，如图 2 所示。

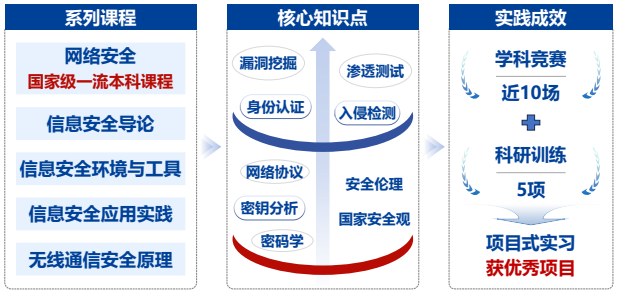


图 2 教学改革成效

如表 1 所示，在项目式实习方面，与中孚、幻尔等科技公司共建多项校企联合工程项目，建立南京中孚信息数据安全“项目式”实习基地，为 203 人次提供企业级实践机会。先后完成“面向车联网安全通信的音频隐写方法研究”、“基于控制屏障函数的 ROSLander 无人车机械臂安全控制方法研究与部署”等项目，将网络安全理论延伸至工控系统与智能装备安全领域，在真实业务场景中开展安全机制设计、系统部署与攻防验证，项目获评优秀项目，指导教师获评优秀指导教师奖，体现出产教融合机制在打通课堂学习到产业实战的实效性，验证了学生在复杂工程环境下的系统安全设计能力与团队协作素养。

如表 2 和表 3 所示，在学科竞赛与科创训练双线并进的培养模式下，学生依托课程训练的攻防实战能力，在全国大学生信息安全与对抗技术竞赛和中国高校计算机大赛网络技术挑战赛等高水平赛事中屡获佳绩，覆盖密码学攻防、网络渗透等多维技术方向；同步开展一系列科创训练项目，提升了学生在动态对抗场景下的复杂工程问题解决能力与创新实践素养，验证了赛课融通机制在激发学生内生动力与提升实战水平方面的有效性。

表 1 项目式实习学生参与情况统计

项目名称	参与人次
无人机入侵检测系统	2
无人车路径规划与避障系统	4
基于控制屏障函数的 ROSLander 无人车机械臂安全控制方法研究与部署	6
云原生研发效能管理平台	5
联邦学习云计算平台	5

表 2 学科竞赛获奖统计

竞赛名称	所获奖项
全国大学生信息安全与对抗技术竞赛	全国一等奖、二等奖
中国高校计算机大赛网络技术挑战赛	全国特等奖、三等奖
中国机器人及人工智能大赛	省级一等奖、全国三等奖
全国大学生信息安全竞赛	全国优胜奖

表 3 科创训练项目立项情况

科创项目名称	级别
基于分层架构的安全强化学习研究	校级
基于强化学习的智能体安全探索应用研究	校级
面向车联网安全通信的音频隐写方法研究	省级
基于强化学习的自适应网络入侵检测技术研究	校级
基于强化学习的空地跨域身份认证系统设计与实现	省级

5 结束语

本文立足网络安全课程教学中内容、方法与能力三重滞后困境，通过产教融合打通产业技术资源向教学资源转化的通道，通过赛课融通建立竞赛对抗压力向学习动能转化的机制，形成了纵向分层递进、横向双轮驱动的立体化育人体系。实践验证表明，科创训练、学科竞赛与项目式实习的系统嵌入，有效弥合了理论讲授与工程实践之间的断层，重塑了静态验证实验向动态攻防对抗的转型路径，推动了单一知识考核向多维能力认证的评价升级，为应用型网络安全人才培养提供了可落地的改革范式与可推广的实施路径。

下一步改革将围绕三大深化方向展开：一是拓展产教融合的行业纵深，面向航空装备智能化与低空经济发展需求，将机载网络安全等低空特色攻防场景纳入实践教学体系；二是固化赛课融通的制度成果，建立竞赛赛题向教学案例转化的标准化流程，形成覆盖低空物联网安全等方向的模块化案例库与自适应训练平台；三是完善能力导向的评价体系，构建涵盖技术能力、工程伦理与团队协作的多维评价指标，推动网络安全人才培养从阶段性改革向制度化、长效化演进，持续为网络强国战略输送高层次应用型安全人才。

参 考 文 献

[1] 邱朋飞.“六维合一”教学模式改革与实践研究——面向网络空间安全国家急需高层次实战化人才培养[J].工业和信息化教育,2024,(9):19-24+30.

[2] 姚川,许力.“思政、科教、实践”多元协同网络空间安全人才培养模式探索[J].计算机教育,2025,(1):22-27.

[3] 马立平,范岩,张海燕.“产教赛融合”模式下计算机基础课程教学模式研究[J].计算机时代,2025,(7):89-93.

[4] 王金双,黄钊,周振吉,等.信息安全专业综合实践课程改革[J].计算机教育,2026,(5):43-47.

[5] 徐曼,张传林,王真,等.面向应用型人才培养的“产教融合+课赛结合”操作系统实践教学改革[J].计算机教育,2026,(5):92-98.

[6] 马瑞强,郭亚楠,孙赛格,等.数据匿名化攻防赛驱动的安全教学改革研究[J].计算机技术与教育学报,2026,14(2):58-62.

[7] 范嘉豪,孙亚楠.“竞赛驱动，科产教融合”的计算机类人才培养模式创新[J].计算机技术与教育学报,2026,14(2):137-142.

[8] 宋斌,张志勇,梁晗.人工智能赋能多模态大模型安全产教协同育人创新实践[J].计算机技术与教育学报,2026,14(3):8-14.