

数智驱动的研究生网络安全防御课程教学创新与实践

付钰¹ 孟庆锐¹ 顾太平² 严博¹

1 海军工程大学信息安全系

2 武昌工学院智能制造学院

DOI:10.32629/mef.v9i7.21422

[摘要] 数智技术迭代重塑网络攻防格局,对高层次网络安全人才的实战能力、创新素养与科研思维提出更高要求。针对《网络安全防御》研究生课程生源基础差异大、内容更新滞后、高阶创新培育不足等问题,本文构建“差异化分层教学、AI全流程赋能、研战科创融合”三位一体教学体系。依托动态学情画像、模块化分层课程与AI智能攻防靶场,搭建科教融汇、实战赋能的闭环育人机制。实践表明,该模式打破同质化教学模式,推动教学从知识灌输转向精准能力培育、被动学习转向主动科研创新,显著提升研究生攻防实战与科研创新能力,可为高层次实战型网络安全人才培养提供可借鉴范式。

[关键词] 研究生教育; 网络安全防御; 一人一案; AI赋能; 创新素质培养

中图分类号: G41 **文献标识码:** A

Digital Intelligence-Driven Teaching Innovation and Practice for Postgraduate Cybersecurity Defense Courses

Yu Fu¹ Qingrui Meng¹ Taiping Gu² Bo Yan¹

1 Department of Information Security, Naval University of Engineering

2 School of Intelligent Manufacturing, Wuchang Institute of Technology

[Abstract] The iteration of digital intelligent technologies has reshaped cyberspace confrontation, putting forward higher requirements for the practical competence, innovative literacy and research thinking of high-level cybersecurity talents. Aiming at the problems of diverse student foundations, outdated curriculum content and inadequate high-level innovation training in the postgraduate course Network Security Defense, this paper constructs a three-in-one teaching system integrating differentiated hierarchical teaching, full-process AI empowerment, and integration of scientific research and practical training. Relying on dynamic learning portraits, modular hierarchical curriculum and AI-based intelligent offensive and defensive shooting range, it establishes a closed-loop talent cultivation mechanism combining scientific research and practical teaching. Practical results show that the proposed model breaks the homogeneous teaching mode, transforms knowledge indoctrination into targeted capability cultivation and passive learning into active scientific research and innovation. It effectively improves postgraduates' practical combat and research capabilities, providing a feasible paradigm for cultivating high-level practical cybersecurity talents.

[Key words] graduate education; cybersecurity defense; individualized training plan for each student; AI empowerment; cultivation of innovative quality

1 引言

数智技术与国家安全体系深度融合,网络空间对抗趋于智能化、体系化、常态化,已成为大国战略竞争核心领域^[1]。当前我国网络安全高层次实战创新型人才缺口持续扩大,传统培养模式与行业高端能力需求存在明显错位。研究生教育是高层次人才培养的关键,承担塑造学生专业体系、科研思维与实战攻防能力的核心任务^[2,7]。《网络安全防御》作为本专业研究生核心

主干课程,衔接基础理论与前沿技术、贯通课堂教学与实战对抗、融合知识学习与科研创新,是培育学生体系化防御思维、复杂场景处置能力与科研攻关素养的重要载体^[3]。

传统教学模式难以适配数智时代网络安全高阶人才培养需求,存在突出结构性矛盾。一是生源差异化与同质化教学不符。研究生生源涵盖本专业保研、跨专业考研、在职攻读等类型,综合能力参差不齐,统一教学易造成“优生吃不饱、差生跟不上”

的两极分化。二是技术快速迭代与课程内容滞后脱节。智能攻防、APT溯源、大模型安全等前沿技术持续更新,但教材内容固化、更新缓慢,导致课堂教学与行业实战脱节。三是知识灌输模式与高阶能力培育相悖。传统教学侧重理论讲授,忽视体系化思维、实战能力与科研创新素养培养,无法适配高阶人才独立科研、应急处置、技术创新的核心能力要求。

针对上述问题,本文立足研究生高阶育人定位,以数智技术为赋能手段,以研战融通为育人路径,重构课程教学体系,探索适配高层次网络安全人才成长规律的创新教学模式。

2 数智驱动的课程教学改革体系架构

立足“科教融合、能力为本、创新为核”的育人理念,面向网络安全智能化攻防新态势,本文从分层教学、智能赋能、研战融合三个维度构建课程育人体系,破解同质化、滞后化、浅层化难题。



图1 “数智驱动、研战融通”教学改革体系架构

本次改革摒弃单一课堂讲授模式,以数据化学情研判为基础,依托AI技术贯通教学全流程数据,融合课程教师与研究生导师双师资源,联动课堂教学、科研项目、实战对抗、学科竞赛多元育人场景。通过搭建“一人一案”分层教学、AI全流程赋能、研创融合培育三大核心模块,精准匹配不同层次学生成长需求,分层实现基础补齐、能力进阶、科创拔尖的育人目标。同时优化课程内容、导学机制、实训考核、思政育人等关键教学要素,构建精准、智能、实战化的新型课程生态,全方位提升学生实操能力、科研创新能力与国家安全素养。

3 一人一案：基于学情画像的差异化分层教学

研究生教育以个性化探究、创新性研究、专业化发展为核心特征。网络空间安全学科研究方向细分度高,涵盖密码安全、系统防御、云网安全、AI安全等领域,学生研究方向、能力基础、发展目标差异显著。课程构建以多维学情画像、模块化分层内容、双师精准导学为核心的“一生一策”差异化育人体系。

3.1 多维学情画像与动态分层机制

精准学情研判是差异化教学的基础^[4]。课程构建“课前摸底、过程追踪、阶段复盘”全周期学情画像机制,依托智能系统从理论基础、编程实操、攻防能力、科研潜力、学习状态五维量化学生素养,建立可视化个人能力档案。

结合学情数据与科研方向,将学生动态分为三类培养层级:

基础夯实型以跨专业生源为主,侧重补齐网络架构、安全协议、攻防原理等核心基础知识;能力提升型面向具备专业基础的学生,重点强化漏洞分析、风险研判、防御设计与应急处置等综合实战能力;拔尖创新型针对基础扎实、潜力突出的学生,聚焦前沿攻防、APT对抗、体系化防御等方向开展高阶创新培育。同时,依托课堂表现、靶场实操、阶段考核等数据动态更新学籍档案,建立层级升降流转机制,杜绝分层标签固化,为学生提供适配性个性化成长路径。

3.2 模块化柔性课程内容体系

为适配分层育人目标,课程打破传统线性章节架构,重构“核心必修、方向选修、前沿拓展”三级模块化体系。核心必修模块筑牢网络安全基础理论与通用攻防能力;方向选修模块紧扣学生科研方向,开设多类专项安全课程,实现教学与科研精准对接;前沿拓展模块覆盖高阶安全技术内容,适配拔尖学生创新发展需求。

各模块均设置基础、进阶、挑战三级梯度,学生可结合学籍自主选择学习起点,教师配套分层教学任务与考核标准,实现基础夯实、能力提升、创新培育的分层育人成效。

3.3 双师协同精准导学机制

创新搭建双师协同导学机制,推行“一生一方案、一目标、一课题”精准培养模式。研究生导师结合学生科研方向明确培育重点,课程教师定制个性化学习方案、把控学习进度、复盘重难点内容,推动课程学习与科研实践深度融合。

课程设置专属导学时段,针对学生知识短板、实验难点、科研切入开展靶向辅导。同时革新同质化评价模式,以能力提升、思维进阶与创新突破为核心,侧重考核学生成长增量,实现因材施教、精准育人。

3.4 科研资源高效转化路径

为破解课堂教学与前沿科研脱节,将教学团队在智能防御、态势感知、恶意流量识别等方向的在研项目梯度拆解,转化为适配进度的子课题与实训任务,实现科研资源向教学资源高效转化。

课堂引入真实科研问题,引导学生完整参与问题挖掘、需求分析、方案设计、模型构建、仿真验证、迭代优化的全流程,掌握科研方法、建立体系思维,缩短从课堂学习到独立科研的成长周期。

4 AI赋能教学：数智技术驱动教学转型

数智技术的发展为课程的智能化教学改革提供了有力支撑^[5]。针对教学资源固化、实训场景单一、效果评价不精准等问题,依托大语言模型、智能学情分析系统、AI攻防靶场,构建全流程的AI赋能体系,推动教学实施由经验驱动向数据驱动转型。

4.1 自适应学习资源AI精准推送

基于大语言模型搭建自适应资源推送系统,依托学情画像实现个性化资源供给:为低阶学习需求学生推送理论解读、阶梯习题与基础案例,快速补齐知识短板;为中阶学习需求学生推

送实操教程、场景任务与典型方案,强化综合应用能力;为高阶学习需求学生推送前沿论文、攻防战例与高端研究成果,拓宽学术创新视野。同步动态更新配套教学资源,有效解决课程内容滞后问题。

4.2 AI智能攻防靶场构建

攻防演练是本课程实践能力培育的核心环节。针对实践场景固化、对抗性弱等问题,依托自研的AI智能攻防靶场搭建高仿真、动态博弈、可迭代的训练环境^[6]。基于最新漏洞库生成异构拓扑与随机攻击路径,搭载AI智能攻击引擎,模拟渗透入侵、APT攻击、恶意流量等行为,构建高强度对抗环境;智能研判思维短板,自动生成防护方案。通过沉浸式对抗训练,锤炼体系化防御思维与攻防实战能力,打通理论到实践壁垒。

4.3 全过程多元AI评价

打破“一张试卷定成绩”的终结性考核方式,构建AI数据驱动的全过程多元评价体系。通过自动采集理论学习、靶场实操、课堂研讨、科研创新等数据,建立可量化、可追溯的学生个人行为档案。依托大数据分析模型,精准研判漏洞、防御架构、应急响应等短板,为教师动态调整教学策略提供支撑。评价重心由知识记忆转向实战能力、体系思维、创新素养的综合考核,以评价改革倒逼人才质量提升。

5 改革成效与反思

5.1 教学改革成效

本培养模式经三届研究生教学迭代优化,育人成效突出。学生在攻防处置、架构设计、科研研发、论文撰写等核心能力全面提升,课程质量、学科竞赛、论文专利等科创成果稳步增长,创新实战素养显著增强。

教学满意度由改革前75.6%提升至96.3%,个性化分层教学、AI实训、科研赋能等改革举措获得学生广泛认可。同时,该模式已在校内多门研究生课程落地应用,育人理念被多所高校借鉴,形成了可复制、可推广的网络安全高层次人才培养范式。

5.2 存在问题与反思

当前改革仍存在三点待改进:一是个性化育人人力成本较高,分层导学工作量大,制约模式规模化推广,后续将依托AI学情研判等工具降低人工成本;二是AI教学应用深度不足,资源推送、实训评价的精准性有待提升,且需持续校验AI内容安全性,后续将建立抽检反馈与模型迭代机制;三是研战融合资源通用

性偏弱,过度依赖团队自有积累。后续将联合多校共建共享资源库,降低模式推广落地门槛。

6 结语

数智时代对网络空间安全高层次人才培养提出了新要求。本文针对传统课程教学的结构性短板,构建“一人一案、AI赋能、研战融通”创新培养体系,以差异化分层教学解决生源差异问题,依托数智技术革新教学模式,结合科研实战锤炼学生创新实践能力,推动课程教学从单一知识传授,转向能力塑造、思维培育与创新赋能的全方位转型。后续将持续优化分层机制、完善AI教学体系、深化科教与研战融合,不断提升研究生培养质量,为国家网络空间安全领域输送德才兼备、研战兼优的创新型人才。

[参考文献]

- [1]廖湘阳,赵莹莹,王潇,等.研究生分类培养链条构建及其融通创新的逻辑与策略[J].学位与研究生教育,2023(4):1-9.
- [2]鲁辉,王乐,田志宏.方班:网安人才培养新模式探索[J].计算机教育,2025(4):3-5.
- [3]WORKMAN M. A study of cybersecurity education using a present-test-practice-assess model[J].IEEE Transactions on Education,2022,65(1):40-45.
- [4]Chhetri C. Exploring large language model-powered pedagogical approaches to cybersecurity education[C]//Proceedings of the 25th Annual Conference on Information Technology Education. New York: ACM, 2024: 163-166.
- [5]王磊,徐子竞,朱戈,等.生成式人工智能赋能网络安全人才培养的探索研究[J].中国电化教育,2023(9):101-108.
- [6]李君,陈万明,董莉.“新工科”建设背景下人工智能领域研究生培养路径研究[J].学位与研究生教育,2021(2):29-35.
- [7]田志宏,王乐,鲁辉,等.创新网络安全人才培养体系,支撑网络强国建设[J].中国网信,2023(9):27-31.

作者简介:

付钰(1982--),女,汉族,博士,湖北武汉人,教授博导,从事网络空间安全教学与科研工作。

孟庆锐(1988--),男,湖北襄阳人,讲师、硕士。

顾太平(1977--),男,安徽滁州人,讲师、博士。

严博(1984--),男,江西丰城人,讲师、博士。