融合人工智能、指挥控制理论与课程思政的高校网络安全攻防实训课程体系规划研究

李千目 [1,2]

1. 塔里木大学 网络安全学院，中国 ·新疆 阿拉尔 843300

2. 南京理工大学 计算机科学与工程学院，中国 ·江苏 南京 210094

摘要：在数字经济快速发展的背景下，高校网络安全专业人才培养面临应对复杂网络安全事件、提升协同处置能力的严峻挑战。指挥控制理论作为统筹协调、精准施策的经典理论，其核心思想与网络安全领域的应急响应、态势感知、协同防御等核心能力要求高度契合。本文基于指挥控制理论的感知、判断、决策、执行、反馈等闭环逻辑，结合高校网络安全专业人才培养目标，从课程目标定位、内容体系构建、实训模式设计、课程思政融合及育人闭环保障五个维度，构建兼具专业性与实践性的高校网络安全专业课体系。通过将指挥控制思想深度融入课程各环节，强化学生的系统思维、协同能力与责任担当，实现从知识传授到能力培养、价值塑造的有机统一，为高校培养适应国家网络安全战略需求的复合型人才提供可行路径。

关键词：指挥控制理论；高校网络安全专业；课程设计；实训教学；育人闭环；课程思政

Research on the Planning of the Training Course System of Cybersecurity Attack and Defense in Universities Integrating Artificial Intelligence, Command & Control Theory and Political Education

Li Qianmu[1,2]

1. School of Cybersecurity, Tarim University, China Xinjiang Aral 843300

2. School of Computer Science and Engineering, Nanjing University of Science and Technology, China Jiangsu Nanjing 210094

Abstract: Under the background of the rapid development of the digital economy, Colleges and universities are encountering significant challenges in cyber security education, including the need to adapt curricula to rapidly evolving threats and to enhance collaborative incident response capabilities. As a classic theory for overall coordination and precise policy implementation, command and control theory is highly consistent with the core capability requirements in the field of cyber security, such as emergency response, situational awareness, and collaborative defense. Based on the closed-loop logic of "perception-judgment-decision-execution-feedback" of command and control theory, combined with the training objectives of cyber security professionals in colleges and universities, this paper constructs a a professional and practical cyber security course system from five dimensions: curriculum objective positioning, content system construction, training mode design, curriculum ideological and political integration, and education closed-loop guarantee. Through the comprehensive integration of command and control principles across all aspects of the curriculum, students' systematic thinking, collaborative skills, and sense of responsibility are significantly enhanced., realizes the organic unity from knowledge imparting ability training and value shaping, and provides a feasible path for colleges and universities to cultivate compound talents that meet the national cyber security strategic needs.

Keywords: Command & control theory; Cyber security major; Curriculum design; Practical training teaching; Education closed loop; Curriculum ideological and political education

0 引言

随着网络空间成为国家主权的新疆域，网络安全已上升为国家战略。根据最新数据，到 2027 年，中国对网络安全专业人员的需求预计将达到 27 万，显示出对高素质网络安全专业人才的迫切需求。目前，网络安全领域技术工人的短缺是由于新技术的快速发展和对在线安全的日益关注

造成的。高校作为网络安全人才培养的主阵地，其专业课设计直接决定人才培养质量。当前，高校网络安全专业课多以技术传授为核心，侧重单一安全技术的讲解与实践，存在课程体系碎片化、学生系统思维缺失、应对复杂网络安全事件能力不足等问题。复杂网络安全事件往往涉及多领域、多环节，需要具备统筹协调、精准决策、协同处置的综合能力，传统课程模式已难以满足这一需求。

指挥控制理论源于军事领域，核心是通过信息获取、分析判断、决策制定、执行反馈的闭环流程，实现对复杂系统的有效管控。该理论所蕴含的系统思维、闭环管理、协同联动等思想，与网络安全领域的态势感知、应急响应、协同防御等核心能力要求高度契合。将指挥控制理论融入高校网络安全专业课程设计，能够有效破解传统课程的局限性，推动课程体系从“技术碎片化”向“系统一体化”转变，从“单一技能培养”向“综合能力提升”转变。本文基于指挥控制理论核心逻辑，结合高校人才培养规律，构建凸显指挥控制思想、强化实训教学、融入课程思政的专业课体系，形成“理论学习—实践锻炼—价值塑造—反馈提升”的育人闭环，为培养适应国家战略需求的网络安全复合型人才提供支撑。

1 指挥控制理论与高校网络安全专业的适配性分析

指挥控制理论核心为“感知、判断、决策、执行、反馈”闭环流程，本质是通过信息高效流转与精准管控，实现复杂系统的有序协调与控制，涵盖信息感知、决策协同与闭环反馈三大要素，强调系统思维、协同联动与动态优化，与网络安全人才能力需求高度契合。

高校网络安全专业需培养具备技术能力、系统思维、协同能力与责任担当的复合型人才，具体包括态势感知、决策处置、协同联动、优化提升及责任担当五大能力。

指挥控制理论与该专业的适配性体现在三方面：逻辑层面，“感知、判断、决策、执行、反馈”与网络安全事件处置流程一致；能力层面，强化系统思维、协同与动态优化能力，弥补传统课程不足；目标层面，均致力于复杂系统的有效管控，实现理论与实践的相互支撑。

2 基于人工智能、指挥控制理论与课程思政的高校网络安全专业攻防实训课程设计框架

本文基于指挥控制理论核心逻辑，结合高校网络安全专业人才培养目标，构建“1-5-3”课程设计框架：“1”个核心引领（指挥控制理论），“5”大设计维度（目标、内容、实训、思政、闭环），“3”个能力层级（基础能力、核心能力、综合能力），实现理论学习、实践锻炼与价值塑造的有机统一。

2.1 课程目标定位：锚定“三维能力”培养

以指挥控制理论为引领，明确课程的“知识、能力、价值”三维目标，突出指挥控制思想对能力培养的深度赋能。一是知识目标，要求学生掌握指挥控制理论核心内涵、网络安全核心技术（如加密技术、入侵检测、应急响应等）、网络安全法律法规等知识，构建“理论 + 技术”的复合型知识体系；二是能力目标，聚焦指挥控制闭环逻辑，培养学生的态势感知能力、决策处置能力、协同联动能力与动态优化能力，实现从单一技术应用到综合系统管控的能力跨越；三是价值目标，融入课程思政元素，强化学生的国家网络安全意识、责任担当与职业道德，树立“网络安全为人民，网络安全靠人民”的价值理念。

2.2 实训课程内容体系构建：遵循“闭环逻辑”，整合“模块内容”

基于指挥控制“感知—判断—决策—执行—反馈”闭环逻辑，将课程内容整合为五大核心模块，实现内容体系的系统性与连贯性。各模块既相互独立又紧密关联，形成“理论铺垫—技术应用—综合实践”的递进式内容结构。

一是感知模块：网络安全态势感知。对应指挥控制的“感知”环节，主要内容包括网络安全数据采集技术（如流量采集、日志分析、漏洞扫描等）、态势感知平台搭建与应用、威胁情报获取与分析等。通过本模块学习，使学生具备全面、实时获取网络安全信息的能力，为后续决策处置提供数据支撑。同时，融入“数据安全与隐私保护”思政元素，强调感知过程中的合规性与责任感。

二是判断模块：网络安全风险分析。对应指挥控制的“判断”环节，主要内容包括网络安全风险评估方法、攻击行为分析技术、漏洞利用机理、风险等级划分标准等。通过本模块学习，使学生能够基于感知信息精准判断安全风险类型、等级与影响范围，形成科学的分析判断能力。融入“批判性思维与严谨治学”思政元素，培养学生严谨的分析态度与科学的判断方法。

三是决策模块：网络安全策略制定。对应指挥控制的“决策”环节，主要内容包括网络安全防护策略设计（如访问控制策略、加密策略、入侵防御策略等）、应急处置方案制定、资源统筹协调方法等。通过本模块学习，使学生能够基于风险分析结果，制定科学、可行的安全策略与处置方案，具备统筹协调的决策能力。融入“全局思维与责任担当”思政元素，培养学生从整体出发解决问题的系统

思维与守护网络安全的责任意识。

四是执行模块：网络安全协同处置。对应指挥控制的“执行”环节，主要内容包括网络安全应急响应流程、攻击阻断技术、数据恢复技术、跨团队协同配合机制等。通过本模块学习，使学生能够精准执行安全策略与处置方案，与团队成员协同配合完成安全事件处置任务。融入“团队协作与敬业精神”思政元素，强调团队协同的重要性与敬业奉献的职业素养。

五是反馈模块：网络安全体系优化。对应指挥控制的“反馈”环节，主要内容包括安全事件处置效果评估方法、防护体系漏洞复盘、安全策略优化技术、持续改进机制构建等。通过本模块学习，使学生能够总结处置经验，发现防护体系不足，动态优化安全策略与防护体系，形成持续提升的能力。融入“精益求精与创新精神”思政元素，培养学生不断改进、勇于创新的进取意识。

2.3 实训模式设计：凸显“实战导向”，构建“层级实训”

基于指挥控制理论的实践属性，构建“基础实训—核心实训—综合实训”三级实训模式，强化实训教学的针对性与实效性，实现从“模拟实践”到“实战锻炼”的过渡。

一是基础实训：聚焦单一环节能力培养。对应五大内容模块，设计针对性的基础实训项目，如“网络安全数据采集实训”“风险评估实训”“防护策略设计实训”等。通过虚拟仿真平台搭建模拟场景，让学生独立完成单一环节的实践任务，夯实基础能力。例如，在感知模块实训中，让学生利用 Wireshark、Snort 等工具采集网络流量数据，分析其中的攻击行为，培养态势感知基础能力。

二是核心实训：聚焦闭环流程协同能力培养。以指挥控制闭环逻辑为核心，设计“完整安全事件处置”实训项目，如“校园网黑客攻击应急处置实训”“企业网络数据泄露事件处置实训”等。将学生分为感知组、分析组、决策组、执行组、反馈组，模拟真实安全事件处置团队，完成“感知—判断—决策—执行—反馈”的全流程协同处置。通过该实训，强化学生的系统思维与协同能力，熟悉闭环处置流程。

三是综合实训：聚焦实战能力提升。引入真实网络安全场景与行业资源，与网络安全企业、公安部门合作，开展“实战化演练”“攻防对抗大赛”等实训活动。例如，联合企业搭建真实的网络安全攻防场景，让学生参与真实的漏洞挖掘、攻击防御任务；组织学生参与国家级、省级网络安全竞赛，以赛促学、以赛促练。通过实战化实训，提升学生应对复杂网络安全事件的实战能力，缩短与行业需求的差距。

2.4 课程思政融合：贯穿“闭环全程”，实现“价值塑造”

将课程思政元素深度融入课程各环节，实现“知识传授、能力培养、价值塑造”的有机统一。一是在理论教学中融入思政元素，通过讲解国家网络安全战略、网络安全领域典型案例（如网络攻击对国家关键信息基础设施的危害、网络安全工作者守护国家网络安全的先进事迹），强化学生的国家网络安全意识与责任担当；二是在实训教学中融入思政元素，通过团队协作实训培养学生的集体荣誉感与协作精神，通过实战化实训强化学生的敬业精神与职业道德；三是在考核评价中融入思政元素，将学生的责任意识、协作能力、合规意识等纳入考核指标，引导学生树立正确的价值观。

2.5 育人闭环保障：构建“反馈 – 优化”机制，提升培养质量

借鉴指挥控制的闭环反馈逻辑，构建“教学实施—效果评估—反馈优化—持续提升”的育人闭环保障机制，确保课程设计的科学性与实效性。一是教学实施环节，通过课堂教学、实训教学以及线上线下融合教学等多种方式，落实课程内容与培养目标；二是效果评估环节，构建“过程性考核 + 终结性考核 + 实战考核”的多元化考核体系，其中，过程性考核关注学生的学习态度与基础能力，终结性考核关注学生的综合知识掌握情况，实战考核关注学生的实战能力与价值素养；三是反馈优化环节，通过学生评价、教师反思、行业调研以及毕业生跟踪等多种渠道，收集课程设计与教学实施中的问题与建议，有针对性地优化课程内容、实训项目与教学方法；四是持续提升环节，将优化后的方案应用于后续教学，形成“实施—评估—反馈—优化”的持续提升闭环，不断提升人才培养质量。

3 结语

指挥控制理论的闭环逻辑、系统思维和协同思想与高校网络安全专业人才培养需求契合，为专业课设计提供理论指导。本文构建了基于人工智能、指挥控制理论和课程思政的课程体系，以“感知、判断、决策、执行、反馈”闭环为核心，整合五大内容模块，建立三级实训模式，融入思政元素，形成育人闭环机制，实现理论学习、实践锻炼与价值塑造的统一。该设计强化学生系统思维、协同能力和实战能力，提升人才培养质量，为培养国家网络安全战略所需复合型人才提供路径。未来通过深化产教融合、

技术赋能和拓宽国际视野，可完善课程体系，提升人才培养针对性和实效性。

参考文献：

[1] 徐慧慧，石章松，吴中红等. OBE 理念下无人指挥与控制技术课程思政探索[J]. 高教学刊，2025,11(11):181-184.

[2] 雷洪涛，袁雪美，朱承等. 混合式教学模式下指挥控制原理课程思政教学改革与实践[J]. 军事高等教育研究，2025,48(01):69-75.

[3] 李千目. 以全新视角审视教育科技与人才的关系[J]. 中国教育网络，2024,(05):36-37.

[4] 李千目. 运用大数据破解教育变革难题[J]. 中国教育网络，2023,(08):71-73.

[5] 陈文娟. 计算机专业课课程思政教学的探索与实践[J]. 中国新通信，2025,27(17):80-82.

课题项目：中国指挥与控制学会教学立项课题（重点课题，编号 2025-XKJS-j04）、江苏省高校“人工智能通识教育教学改革研究”专项课题（重点课题，编号 2025AIGE004）资助。

作者简介：李千目（1979-），男，安徽人，教授、博导。