Advances in Education 教育进展, 2026, 16(8), 1852-1858
Published Online August 2026 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2026.1681824

Hans汉斯

AIGC赋能网络空间安全课程群教学模式创新研究

——以Python网络编程教学为例

饶哲恒

杭州电子科技大学网络空间安全学院，浙江 杭州

收稿日期：2026年7月19日；录用日期：2026年8月20日；发布日期：2026年8月27日

摘　要

针对网络空间安全课程群教学中知识割裂、编程与安全脱节、实验环境复杂和个性化指导缺失等痛点，提出一种AIGC赋能的教学创新模式。该模式以“大模型驱动、课程群协同、案例式牵引”为核心理念，构建了智能代码生成、数据包分析可视化、攻防场景模拟和个性化调试指导四维能力框架，并以Python网络编程为枢纽课程，在Socket编程、Scapy协议分析、网络扫描、协议实现与安全加固、红蓝对抗和综合项目六大模块中实现系统化落地。提出了一种将脚手架理论应用于AIGC辅助教学的阶梯式撤除实施模型，通过智能代码辅助的渐进式撤除机制平衡AIGC辅助与学生自主能力培养。教学实践表明，该模式可有效提升学生的协议理解深度和安全编程实战能力，强化课程群跨模块知识迁移效果。

关键词

AIGC，网络空间安全，课程群，Python网络编程，教学模式，大语言模型，攻防实训

A Study on the Innovative Teaching Model of AIGC-Empowered Cybersecurity Course Cluster

—Taking Python Network Programming Teaching as an Example

Zheheng Rao

School of Cyberspace, Hangzhou Dianzi University, Hangzhou Zhejiang

Received: July 19, 2026; accepted: August 20, 2026; published: August 27, 2026

文章引用: 饶哲恒. AIGC 赋能网络空间安全课程群教学模式创新研究[J]. 教育进展, 2026, 16(8): 1852-1858.
DOI: 10.12677/ae.2026.1681824

Abstract

Addressing the pain points in cybersecurity course cluster teaching, such as knowledge fragmentation, a disconnect between programming and security, complex experimental environments, and lack of personalized guidance, this paper proposes an innovative teaching model empowered by AIGC. This model, with "large-scale-model-driven, course-cluster collaboration, and case-based guidance" as its core concepts, constructs a four-dimensional capability framework encompassing intelligent code generation, packet analysis visualization, attack and defense scenario simulation, and personalized debugging guidance. Using Python network programming as the hub course, it is systematically implemented in six modules: Socket programming, Scapy protocol analysis, network scanning, protocol implementation and security hardening, red-team/blue-team exercises, and comprehensive projects. A tiered-fading implementation model is proposed, applying scaffolding theory to AIGC-assisted teaching. This gradual-fading mechanism of intelligent code assistance balances AIGC support with the cultivation of students' self-directed learning abilities. Teaching practice shows that this model can effectively improve students' depth of protocol understanding and practical security programming skills, and enhance the cross-module knowledge transfer effect of the course cluster.

Keywords

AIGC, Cybersecurity, Course Cluster, Python Network Programming, Teaching Model, Large Language Model, Attack and Defense Training

1. 引言

网络空间安全自 2015 年获批一级学科以来，国内 200 余所高校相继开设本科专业，逐步建成以计算机网络、Python 网络编程、密码学、渗透测试为核心的课程群育人体系。该学科兼具理论密集、技术迭代迅速、实战性极强的特征，对学生跨课程知识融合能力、代码实操能力、攻防场景研判能力提出了较高要求[1]。

传统课程群教学存在四大结构性短板，制约实战型人才培养质量。一是课程体系碎片化，各课程独立授课、知识点壁垒明显，计算机网络协议理论与 Python 编程实操脱节，学生难以形成“理论解析–代码复现–安全验证”的完整思维链路[2]；二是编程教学场景适配度低，通用型 Python 教学案例无法匹配漏洞挖掘、流量分析、端口探测等网安专属场景，学生编程能力难以向安全实战迁移[3]；三是攻防实训环境运维成本高，环境部署、依赖配置、故障排查占用大量课时，有效实训时长不足[4]；四是大班教学个性化指导缺失，师生配比失衡导致学生代码调试、协议解析难题无法得到及时精准指导[5]。

以 GPT-4o、Claude 为代表的多模态大语言模型，具备高质量代码生成、语义推理、场景仿真、交互式答疑能力，为破解网安教学痛点提供了全新技术路径。当前学界关于 AIGC 赋能编程教学的研究多聚焦单门课程的单点应用，主要集中在代码辅助生成、课后答疑、作业批改等浅层场景，尚未将 AIGC 作为课程群知识协同融合的核心纽带，缺少适配网络空间安全攻防实训场景的系统化教学框架，同时缺乏可落地的 AI 辅助教学管控机制与阶梯式能力培养方案。

基于此，本文以 Python 网络编程为枢纽课程，依托 AIGC 技术搭建课程群协同教学体系，构建四维智能赋能能力矩阵，引入脚手架教学理论设计阶梯式 AI 辅助撤除模型，详细阐述核心提示词设计方案、安全过滤机制与技术实施流程，通过教学实践验证模式有效性，精准界定本文创新边界，为网安专业 AIGC 深度育人提供理论支撑与实践参考。

2. 网络空间安全课程群教学痛点分析

2.1. 课程群内知识壁垒突出，体系化能力缺失

网络空间安全课程群各课程逻辑关联紧密，但传统分科教学模式造成严重的知识割裂。计算机网络课程侧重 TCP/IP 协议原理、网络拓扑、拥塞控制等理论讲解，学生仅能通过可视化工具被动观测数据包，无法通过 Socket、Scapy 自主完成协议构造、解析与篡改；密码学课程聚焦加密算法数学原理，却未对接网络通信实战，学生难以实现 Python 环境下的加密通信、TLS 安全套接字搭建。课程间的知识断层，导致学生单科考核达标，但面对跨课程综合攻防任务、安全工具开发任务时无从下手，无法形成系统化的网安实践能力。

2.2. 编程教学场景单一，与网安核心需求脱节

传统 Python 编程教学以通用能力培养为目标，教学案例多为基础算法、数据管理系统、普通爬虫开发，完全脱离网安专业核心能力需求。教学体系缺少原始套接字编程、自定义数据包构造、端口扫描开发、流量异常分析、安全漏洞脚本复现等专项训练内容。学生掌握基础语法后，不具备安全编程思维与攻防场景适配能力，进入高阶网络安全、渗透测试课程后，需要重新学习安全专属编程技能，知识迁移效率极低，严重影响人才培养连贯性。

2.3. 实训环境运维繁琐，实战教学效率低下

网安攻防实训高度依赖专属仿真环境，传统线下实训存在部署复杂、兼容性差、故障频发、场景固化等问题。端口扫描、协议攻防、红蓝对抗等实验需要独立配置网络规则、靶机环境与访问权限，大量课时消耗在环境调试与问题排查中，有效实操训练时长被严重压缩。同时，传统实训环境更新滞后，无法适配新型网络攻击手段与行业攻防场景迭代，难以满足高阶实战教学与学科竞赛训练需求。

2.4. 大班教学资源有限，个性化育人难以落地

当前高校网安专业普遍存在大班授课、师生比失衡的问题，教师无法兼顾不同层次学生的学习进度与知识短板。基础薄弱学生在代码调试、场景实操中积累大量问题，无法及时纠错提升；能力突出学生缺少高阶拓展训练资源，创新能力与竞赛潜力难以释放，传统教学模式无法实现分层化、个性化、精准化育人。

3. AIGC 赋能教学框架设计

3.1. 设计理念与总体架构

本文教学框架秉持三大核心设计理念：大模型驱动，依托主流大语言模型的代码生成、语义推理、多轮交互能力，突破传统师资与实训资源局限；课程群协同，以 Python 网络编程为枢纽，借助 AIGC 跨课程语境适配能力，打通计算机网络、密码学、网络安全、渗透测试的知识壁垒，实现理论、编程、攻防实战的递进式融合；案例式牵引，所有 AI 交互场景与实训任务均基于真实网安攻防场景设计，兼顾教学基础性与行业实战性。

整体采用三层闭环架构，依次为基础设施层、四维 AIGC 能力层、教学应用层。基础设施层包含多大模型 API 适配模块、网安课程专属知识库、Docker 容器化隔离实训平台与安全过滤模块，为智能教学提供底层技术支撑；四维 AIGC 能力层集成智能代码脚手架、数据包可视化分析、攻防场景模拟、个性化引导调试四大核心能力；教学应用层对接六大 Python 网络编程实训模块，落地阶梯式教学、实战实训、个性化答疑等育人功能，实现技术赋能与教学场景的深度绑定。

3.2. 四维 AIGC 能力矩阵

(1) 智能代码生成与阶梯式脚手架。将每项编程任务设计为四个递进层级：Level 1 完整脚手架。AIGC 生成完整参考代码，学生阅读理解并复现；Level 2 部分脚手架。仅提供函数签名和接口文档，学生补充实现体；Level 3 最小脚手架。仅提供需求规格，学生独立设计编码；Level 4 无脚手架。学生自主拓展优化，AIGC 仅作为按需代码审查助手。该设计对应 Bloom 认知层次，确保 AIGC 服务于编程能力的实质性增长。所有生成代码经“安全过滤器”审查，过滤硬编码凭据和危险系统调用。

(2) 数据包分析智能可视化。学生将 Scapy 捕获的 PCAP 数据提交 AIGC，系统逐字段解码协议层次(Ethernet→IP→TCP/UDP→应用层)，标注字段语义和异常模式(异常标志位组合、非标准端口通信)，并自动生成 Python 可视化代码绘制协议交互时序图和通信拓扑图。将传统对照 RFC 逐字节解码的低效过程转化为即时的、语义化的协议学习体验。

(3) 攻防场景自动化模拟。AIGC 充当“自动化红蓝对抗引擎”：红队角色中，根据教学主题自动生成参数可变的攻击脚本(SYN Flood、慢速连接耗尽、畸形包注入等)并在沙箱中执行；蓝队角色中，对攻击效果进行结构化分析，解释协议层面的防御弱点根因并建议加固策略。所有攻击代码严格限制在 Docker 隔离环境中，通过 iptables 阻断外部网络访问。

(4) 个性化调试指导。基于苏格拉底式教学对话：AIGC 不直接给出答案，而是通过多轮提问引导学生自主定位问题。描述预期与实际行为的差异→检查相关协议字段→添加诊断性输出→最小化修复提示。提示词被设计为“导师”角色，坚持“三分提示、七分引导”策略。针对高频错误建立模式库，实现快速精准的引导式诊断。

3.3. 核心技术实施细节补充

(1) 典型教学场景提示词范例与设计思路

为保障 AIGC 赋能教学的规范性、针对性与可复制性，本文针对概念解释、代码纠错、方案设计三大核心教学场景，设计标准化专属提示词，兼顾引导性、专业性与安全性，具体范例如下。

场景一：协议概念深度解析(适配低年级理论实训)。提示词内容：“你现在是网络空间安全专业 Python 网络编程课程专任教师，采用启发式教学方式，为学生讲解 TCP 三次握手协议原理。结合 Socket 编程实战场景，区分理论流程与代码实现差异，不直接灌输结论，通过分层提问引导学生理解协议字段作用，输出通俗易懂、贴合课程知识点的讲解内容，禁止输出超纲内容与高危技术原理。”设计思路：聚焦理论落地难点，弱化纯理论说教，对接编程实战，启发学生自主思考，适配课程群协同教学需求。

场景二：代码纠错与引导调试(适配实操训练)。提示词内容：“请以教学辅导身份排查学生 Python 网络编程代码错误，仅提供排查思路与关键提示，不直接输出完整修正代码。结合网络协议原理分析报错根因，标注代码逻辑漏洞、协议适配错误、语法缺陷，分步骤引导学生自主调试，同时规避高危操作指导，适配本科实训教学场景。”设计思路：严格贴合阶梯式脚手架撤除模型，保留学生自主操作空间，杜绝 AI 代做，兼顾纠错效率与能力培养。

场景三：攻防实训方案设计(适配高阶综合项目)。提示词内容：“基于 Python Scapy 工具，设计一套

合规可控的 DNS 数据包解析与异常检测实训方案，包含实训目标、代码框架、实验步骤、风险规避要点与防御思路。所有实训内容仅限教学隔离环境使用，禁止提供可直接对外攻击的完整脚本，重点体现协议安全原理与攻防博弈逻辑。”设计思路：兼顾实战性与安全性，聚焦方案设计思维培养，规避技术滥用风险，适配网安专业实训规范。

(2) 安全过滤器技术选型与工作流程

本文安全过滤器采用规则匹配与静态代码分析融合技术方案，轻量化、高效率，适配教学场景实时筛查需求，核心用于拦截 AIGC 生成的高危、违规代码，防范教学风险。技术选型层面，规则匹配模块依托网安教学高危脚本特征库，收录恶意端口扫描、DDoS 攻击、越权访问、硬编码密钥等违规特征；静态分析模块通过 AST 抽象语法树解析代码结构，识别高危系统调用、网络非法连接、权限篡改等风险行为。

完整工作流程：第一步，AI 生成初始代码文本；第二步，安全过滤器对代码进行特征匹配筛查，初步拦截高危特征语句；第三步，通过静态语法分析遍历代码逻辑，识别隐性风险行为；第四步，无风险代码正常输出展示，高危代码自动拦截、脱敏处理，并同步提示风险类型与教学规避原因；第五步，留存筛查日志，用于教学复盘与风险溯源。

4. Python 网络编程教学模块化实践

4.1. Socket 编程基础：阶梯式脚手架分层训练

以“多客户端并发聊天服务器开发”为核心实训项目，全面落地四级阶梯式脚手架撤除模型。Level 1 阶段，AI 生成带完整注释的 TCP 回声服务器代码，学生复现运行，掌握 Socket 核心 API、网络通信基础逻辑；Level 2 阶段，仅提供客户端处理函数签名，学生自主实现多线程并发通信功能，AI 在关键逻辑节点提供引导式提示；Level 3 阶段，学生独立完成私聊、群聊、昵称认证、异常断开重连等拓展功能；Level4 阶段，学生自主优化架构，将多线程模型改造为异步 I/O 模型，AI 从线程安全、资源释放、边界容错等维度开展代码审计。

4.2. Scapy 数据包分析：协议可视化赋能实训

以“DNS 查询数据包构造与解析”为实训主题，依托 AIGC 可视化能力破解协议学习难点。学生通过 Scapy 逐层构造以太网、IP、UDP、DNS 协议数据包，针对端口错误、字段缺失、协议层级混乱等常见问题，AI 实现逐层字段校验，精准定位报错节点并给出针对性修正思路。学生完成数据包构造与解析后，AI 自动生成协议交互时序图、数据包层级拓扑图，直观展示 DNS 递归解析完整流程，有效解决协议抽象难懂、实操无从下手的问题。

4.3. 网络扫描技术：攻防双视角场景实训

以“隐蔽端口扫描器开发与防火墙规避”为主线，构建攻防双视角教学场景。进攻视角下，学生先实现 TCP Connect 扫描器，理解全连接扫描的原理与高日志特征，再通过 AI 引导自主编写 SYN 半开扫描代码，掌握隐蔽扫描的技术逻辑与优势；防御视角下，AI 根据扫描行为自动生成 Snort 流量检测规则，帮助学生理解“扫描规避–流量检测”的攻防博弈关系。同时，AI 参数化生成不同防火墙配置的靶机环境，学生通过分析扫描结果反向推理防火墙过滤规则，完成完整的攻防闭环实训，实现编程能力与安全研判能力同步提升。

4.4. 协议实现与安全加固：代码赋能漏洞修复

针对传统教学重协议实现、轻安全加固的短板，依托 AIGC 开展协议安全专项实训。以 HTTP、TCP

协议为载体，学生基于 Python 完成基础协议请求、数据传输代码开发，AI 自动检测代码中存在的明文传输、端口暴露、无异常容错、恶意请求未拦截等安全漏洞，通过阶梯式引导方式，带领学生逐步完成 TLS 加密改造、请求合法性校验、异常捕获加固、访问权限限制等优化操作，让学生掌握“协议开发–漏洞检测–安全加固”的完整流程，打通基础编程与安全防护的知识壁垒。

4.5. 红蓝对抗模拟：容器化闭环攻防实训

依托 AIGC 攻防场景模拟能力与 Docker 隔离环境，开展轻量化红蓝对抗实训。红队实训中，AI 生成参数可控的慢速连接耗尽、畸形 TCP 包注入等轻量化攻击脚本，学生运行脚本并观测网络异常现象；蓝队实训中，学生通过代码抓取流量、分析攻击特征，自主编写流量过滤、异常拦截防护代码，AI 辅助分析防御漏洞、优化防护策略。所有对抗场景均在隔离环境内开展，全程可追溯、可复盘，有效解决传统红蓝对抗场景单一、风险不可控、复盘难度大的问题。

4.6. 综合项目实训：课程群知识融合落地

整合前五模块知识点，设置“轻量化网络安全检测工具开发”综合项目，要求学生融合 Socket 通信、Scapy 流量分析、端口扫描、协议加固等技术，自主完成工具开发。AI 根据学生能力差异提供分层辅助，基础薄弱学生可获取框架性提示，优秀学生可获得高阶功能拓展建议，最终实现课程群跨知识点融合应用，全面检验学生编程能力、协议理解能力与安全实战能力，达成以赛促学、以练促创的育人目标。

5. 挑战与应对策略

5.1. 学术诚信与 AIGC 依赖

学生过度依赖 AIGC 代码生成而丧失独立编程能力是首要风险。应对策略：(1) 过程性评价导向，评分重心转向开发过程记录(对话日志、迭代历史、反思笔记)；(2) 脚手架强制撤除，期末无脚手架测试成绩占总评不低于 30%；(3) 口试答辩机制，每位学生至少完成一次面对面代码走查；(4) AIGC 素养教育，开设专题讲座明确“可为与不可为”边界。

5.2. 模型幻觉与内容准确性

LLM 可能生成虚假 API、错误协议语义或危险编程模式，学生难以甄别。对策：(1) 多模型交叉验证，关键代码经 GPT-4o 和 Claude 异构交叉比对；(2) 教师预审，攻击性代码须经教师审查和沙箱验证后方可发放；(3) 故意植入错误训练，设计专项练习培养学生批判性评估 AI 输出的能力。

5.3. 教师角色重塑

教师需从“知识传授者”升级为“学习体验架构师”。核心工作转为设计提示词模板、策划教学任务链、审核 AIGC 输出质量、设计评价量规、示范如何批判性使用 AIGC。高校应配套开展面向网安教师的 AIGC 教学能力培训，涵盖提示词工程、输出评估方法和 AI 伦理教育。

6. 结论与展望

针对网络空间安全课程群知识割裂、课赛脱节、实训低效、个性化育人不足等教学痛点，本文构建 AIGC 赋能的课程群协同教学创新模式，确立“大模型驱动、课程群协同、案例式牵引”三大核心理念，搭建四维智能赋能技术框架，并在 Python 网络编程六大核心教学模块中完成系统化落地。本文核心创新与研究贡献精准界定为：第一，区别于现有 AIGC 单一课程应用研究，本文首次将 AIGC 定义为网安课程群知识协同融合的核心工具，构建了跨课程、全链路、可落地的数智化教学体系；第二，创新性提出

适配网安实训场景的 AIGC 阶梯式脚手架撤除实施模型，有效平衡智能工具赋能与学生自主能力培养，为 AI 辅助实战化教学提供标准化实施路径；第三，完善了 AIGC 网安教学的技术细节与安全管控机制，补充标准化提示词范例、安全过滤技术流程与隔离实训方案，解决了现有研究重框架、轻落地的问题。

本文前期教学实践仅覆盖少量教学班，样本规模与观测周期有限，教学模式的普适性仍需进一步验证。后续研究将扩大教学实验样本，开展多院校对照教学测试，持续优化阶梯式脚手架模型参数；针对网安教学场景微调专属提示词库，进一步降低模型幻觉误差；搭建校际 AIGC 网安教学资源共享平台，实现提示词模板、实训案例、安全方案的开源共享，持续完善 AIGC 赋能网安实战化育人体系。

基金项目

杭州电子科技大学高等教育教学改革研究项目(YBJG202535)。

参考文献

[1] 施莹娟, 沈才有, 郑秀峰, 等. 实战型网络空间安全人才“三强六阶”递进式人才培养模式探索[J]. 计算机教育, 2025(12): 47-53.

[2] 苏婷, 蒋琳, 房敏. 网络与信息安全方向系列课程贯通式教学探索与实践[J]. 计算机教育, 2023(6): 76-80.

[3] 郭李华. “赛教融合”模式下的网安专业 Python 实践教学研究[J]. 网络安全技术与应用, 2025(4): 118-120.

[4] 李琦, 崔天宇, 肖勇, 等. 面向网络安全专业人才培养的安全大模型实践案例设计[J]. 计算机教育, 2025(9): 19-26.

[5] 郝志强, 刘冬, 刘忻. “四维一体”的 AI 安全人才培养生态系统建设[J]. 中国网信, 2026(2): 47-50.