College and Job 职业教育发展, 2026, 15(9), 250-259
Published Online September 2026 in Hans. https://www.hanspub.org/journal/ve
https://doi.org/10.12677/ve.2026.159388

Hans汉斯

人工智能赋能网络安全能力建设中的人才制约及其应对

鲁先志

重庆电子科技职业大学人工智能与大数据学院(网络空间安全学院)，重庆

收稿日期：2026年8月10日；录用日期：2026年9月3日；发布日期：2026年9月11日

摘　要

人工智能特别是生成式大模型正在重塑网络攻击、防御与安全治理方式，网络安全人才制约也由单纯的数量不足转变为人才总量短缺与能力结构失衡并存。针对复合型实战人才供给不足、人工智能－网络攻防－行业业务能力割裂及培养体系响应迟滞等问题，本文以能力本位教育、项目式学习和情境学习为教学理论基础，并引入组织知识创造理论，构建“能力目标－真实项目－情境参与－知识协同”的分析框架。研究提出，人才培养应由知识叠加转向能力贯通，重点形成将人工智能输出转化为可信安全证据、将技术异常转化为业务风险判断、将攻防结果转化为治理决策的三种能力。基于职业本科的类型定位，进一步提出场景驱动的课程模块开发闭环、项目制虚拟教研室、安全责任分级管理及产教融合实战环境，并与普通应用型本科进行类型化比较。研究认为，上述机制有助于把岗位能力要求转化为可教、可练、可评的项目任务，但其实施仍受真实场景供给、跨专业协作成本、企业参与稳定性、数据合规和实证证据不足等约束，需要通过分级脱敏、制度化协作、周期评价和持续验证加以控制。

关键词

人工智能赋能，网络安全人才，复合型实战人才，职业本科教育

Talent Constraints and Countermeasures in AI-Empowered Cybersecurity Capacity Building

Xianzhi Lu

School of Artificial Intelligence and Big Data (School of Cyberspace Security), Chongqing Polytechnic University of Electronic Technology, Chongqing

Received: August 10, 2026; accepted: September 3, 2026; published: September 11, 2026

文章引用: 鲁先志. 人工智能赋能网络安全能力建设中的人才制约及其应对[J]. 职业教育发展, 2026, 15(9): 250-259.
DOI: 10.12677/ve.2026.159388

Abstract

Artificial intelligence (AI), particularly generative large language models, is reshaping cyberattack, defense, and security governance. The talent constraint in cybersecurity has consequently evolved from a simple quantitative shortage into a compound problem involving both insufficient supply and structural capability imbalance. To address the shortage of interdisciplinary practice-oriented professionals, the fragmentation among AI, cyber offense and defense, and industry-domain capabilities, as well as the slow response of education systems to technological and industrial change, this paper develops an analytical framework of "competency objectives-authentic projects-situated participation-knowledge collaboration" based on competency-based education, project-based learning, situated learning, and organizational knowledge-creation theory. It argues that talent development should shift from knowledge accumulation to capability integration, with emphasis on three transformation capabilities: converting AI outputs into trustworthy security evidence, translating technical anomalies into business-risk judgments, and transforming offensive and defensive findings into governance decisions. Drawing on the distinctive positioning of vocational undergraduate education, the paper further proposes a scenario-driven curriculum-module development cycle, a project-based virtual teaching and research office, graded safety-responsibility management, and an industry-education integrated practice environment, and compares these mechanisms with those of application-oriented undergraduate education. These mechanisms may help convert occupational competency requirements into teachable, trainable, and assessable project tasks; however, their implementation remains constrained by access to authentic scenarios, interdisciplinary collaboration costs, continuity of enterprise participation, data compliance, and limited empirical evidence. These constraints should be addressed through graded de-identification, institutionalized collaboration, periodic evaluation, and continuous validation.

Keywords

AI Empowerment, Cybersecurity Talent, Interdisciplinary Practice-Oriented Talent, Vocational Undergraduate Education

1. 背景与人才需求

随着数字化、智能化进程加速，人工智能特别是生成式大模型正深刻改变网络攻防技术生态。一方面，攻击者借助人工智能开展漏洞探测、钓鱼内容生成、攻击路径优化和恶意代码变异，使网络攻击呈现自动化、精准化、隐蔽化特征；另一方面，防御体系也加快向智能检测、主动研判和自动响应转型，大模型逐步应用于日志分析、威胁识别、攻击溯源与风险预测。网络空间对抗由传统的“人与人、工具与工具”较量，转向模型、数据、平台与专业人员协同的体系化对抗，传统侧重知识传授和单项防御技能的人才培养模式已难以适应新的攻防形势[1]。

我国网络安全专业布局和人才培养规模持续扩大，截至 2024 年 6 月，全国已有 625 所高校开设网络安全相关专业，但人才供给在数量、结构和能力上仍难以满足产业需求，2024 年明确提出实战能力要求的网络安全岗位占比已达到 63% [2]。人工智能时代，产业需要的不再只是掌握安全工具的技术人员，而是能够在真实或高仿真环境中综合运用人工智能、网络攻防和安全数据分析技术，完成威胁检

测、分析研判、应急处置与合规治理，并能够识别模型幻觉、数据泄露和算法攻击等新型风险的复合型实战人才[3]。2024 年，人力资源社会保障部、中央网信办、教育部等九部门联合印发《加快数字人才培育支撑数字经济发展行动方案（2024—2026 年）》，提出围绕人工智能、数据安全等数字领域加强人才培养，全面推行工学一体化培养，深化产教融合，加大复合型数字人才培养力度[4]；国务院《关于深入实施“人工智能+”行动的意见》进一步提出推进产教融合、跨学科培养，强化网络空间信息精准识别、态势主动研判和风险实时处置能力[5]。这既对高校课程体系、师资结构、实战环境和评价机制提出了新挑战，也为信息安全职业本科发挥面向岗位、突出实践和深化产教融合的类型教育优势提供了重要契机。

2. 人才制约：既懂人工智能又懂攻防和业务的复合型人才不足

2.1. 人才总量不足与复合型人才结构性短缺相互叠加

当前，我国网络安全人才供给仍难以匹配网络安全产业快速发展的需要，特别是能够解决真实安全问题的实战型人才供给不足[1] [2]。人工智能进一步推动网络安全产业的岗位边界和能力要求发生变化：传统的安全运维、监测分析、漏洞挖掘和应急响应岗位，开始大量涉及机器学习、智能检测、安全数据分析、大模型应用和自动化响应；人工智能系统本身又催生模型安全测试、数据安全治理、算法风险评估和大模型红队测试等新任务[2] [6] [7]。

因此，当前网络安全人才缺口已不只是“人数不够”，更突出表现为高层次、复合型和实战型人才供给不足。既掌握人工智能技术，又能够进入真实攻防场景、理解行业业务逻辑并承担安全决策责任的人才更为稀缺。人才供给的数量缺口与能力结构缺口相互叠加，成为制约人工智能赋能网络安全能力建设的重要瓶颈。

2.2. 人才能力结构相对割裂，人工智能、攻防与业务能力难以融会贯通

人工智能时代的网络安全岗位已经由单一技术操作转向多技术协同和全生命周期安全保障。工业和信息化部发布的《网络安全产业人才岗位能力要求》将网络安全人才的岗位能力划分为综合能力、专业知识、技术技能和工程实践四个维度，覆盖规划设计、建设实施、运行维护、应急防御和合规管理五个方向，并将业务场景把握、业务需求分析和复杂工程问题处理纳入能力体系[8]。

这意味着复合型网络安全人才不仅要掌握机器学习、数据挖掘和大模型应用，还要具备漏洞分析、渗透测试、攻击研判、日志取证、应急响应和追踪溯源等攻防能力，并能够结合政务、金融、能源、通信和工业互联网等行业业务，判断安全事件的影响范围、风险等级和处置优先级。然而，现实中仍普遍存在“懂人工智能的不熟悉攻击机理和处置流程、懂攻防的不具备模型与数据分析能力、懂技术的不理解业务和合规要求”的能力断层。特别是在大模型安全领域，提示注入、越狱攻击、隐私泄露、模型后门和对抗样本等新型风险，要求测试人员同时具备模型机理理解、攻击思维、安全验证和风险评估能力[7]。单一学科背景和单项工具技能已难以满足智能化、体系化网络攻防的需要[9]-[11]。

2.3. 人才培养体系对产业和技术变化响应不足

现有高校网络安全人才培养仍不同程度存在课程内容更新滞后、理论教学与实战训练脱节、实战师资不足以及实践平台与真实环境差距较大等问题[1] [3] [9]。部分课程仍以传统网络防护、理论验证和单项工具操作为主，对智能攻击、模型安全、AI 辅助威胁研判和人机协同处置等内容覆盖不足；人工智能课程又多侧重算法原理和通用模型训练，缺少网络流量、攻击日志、恶意样本和业务系统等安全场景支撑，学生难以将算法能力转化为网络安全实战能力。

李岷龙构建的数智时代网络安全人才胜任力模型，从专业知识、技术技能、综合能力和实践经验四个维度揭示了网络安全人才的能力构成[10]。但在人工智能赋能网络安全的新形势下，仅具备上述要素仍不足以说明人才能否胜任复合型岗位，还应进一步考察其跨领域转换能力，即能否将人工智能输出转化为安全证据、将攻防发现转化为业务风险判断，并将技术结论转化为可执行的治理措施。由此，复合型人才培养不仅要补充人工智能知识，更要强化不同能力要素在真实任务中的协同运用。

当前，部分校企合作仍停留在讲座、短期培训和一般性实习层面，企业岗位标准、真实业务流程、攻防项目和行业评价要求未能深度进入人才培养全过程，导致部分毕业生虽然掌握若干安全工具，却缺乏在复杂业务环境中开展监测、研判、处置、复盘和持续改进的综合能力[12]-[14]。

3. 理论基础与分析框架

3.1. 能力本位教育与项目式学习的互补

能力本位教育(Competency-Based Education, CBE)强调以岗位胜任要求界定学习成果，并依据可观察的表现证据判断能力是否形成，其价值在于把产业需求、课程目标、项目任务和评价标准建立对应关系。职业教育中的能力不能被窄化为单项操作，而应包含知识、技能、判断、协作和责任在具体职业情境中的综合运用[15]。据此，本文提出的三种转化能力既是培养目标，也是课程设计与考核评价的主线：每一种能力均应对应任务情境、过程记录、成果交付和现场答辩等证据。

项目式学习(Project-Based Learning, PBL)以真实或高仿真的复杂问题组织学习，通过持续探究、协作实施和成果生产促进知识迁移[16]。PBL 为三种转化能力提供任务载体，CBE 则规定任务所要形成的能力标准与达成证据，二者形成“以能力标准确定项目边界、以项目过程生成能力证据”的互补关系。在网络安全教学中，项目不应止于完成一次漏洞利用或模型调用，而应包含数据来源审查、模型输出验证、攻击链分析、业务影响评估、处置方案比较与复盘改进。

3.2. 情境学习与责任递进

情境学习理论认为，学习并非脱离实践共同体的知识接收，而是学习者通过合法的边缘参与逐步走向充分参与的社会过程[17]。这一理论能够解释本文提出的“操作执行者－问题分析者－任务组织者－责任承担者”递进路径：学生先在明确授权和操作规范下完成局部任务，再逐步参与跨角色协作、业务权衡和现场决策，最终在可控条件下对技术结论、业务影响和过程合规承担责任。因而，实战环境既要提供技术对象，也要呈现业务约束、角色关系、审批边界和处置后果。

3.3. 组织知识创造与跨专业协作

人工智能教师、网络安全教师和行业专家分别拥有模型方法、攻防经验与业务规则，跨专业协作的难点并非人员简单组合，而是不同知识能否持续转化和共享。组织知识创造理论强调隐性知识与显性知识通过社会化、外显化、组合化和内隐化循环实现组织层面的创造与扩散[18]。据此，跨专业团队应围绕同一项目开展场景讲述、任务拆解、规范编制、联合实施和复盘沉淀：行业专家将业务经验和失败案例外显为约束条件，教师把分散知识组合成任务工单与评价量规，团队再通过教学实施和企业验证将其内化为可复用的课程能力。

综上，本文形成“能力目标－真实项目－情境参与－知识协同”的理论框架：CBE 回答“培养和评价什么”，PBL 回答“通过什么任务培养”，情境学习回答“如何由参与走向责任承担”，组织知识创造理论回答“跨专业团队如何持续生产和更新教学知识”。三种转化能力位于框架中心，并通过课程、师资、环境与制度四类机制落地。

4. 思路举措与保障条件

4.1. 思路举措

(1) 从知识叠加转向能力贯通培养复合型人才

人工智能时代的复合型网络安全人才，不应被简单理解为同时学习人工智能、网络攻防和行业业务三类知识。三类知识如果相互割裂，学生即使完成了全部课程，也可能无法解决真实安全问题。复合型人才培养的关键，应是提高学生在不同知识领域之间转换信息、建立联系和作出判断的能力。

首先是将人工智能输出转换为安全证据的能力。学生不能只会调用模型生成分析结果，还应能够追溯模型使用的数据、检验分析结论、识别模型幻觉，并通过日志、流量、代码和系统状态对结论进行交叉验证。其次是将技术异常转换为业务风险的能力。学生发现漏洞、异常流量或攻击行为后，应能够进一步判断其影响的业务流程、数据范围、用户群体和服务连续性，而不是把发现技术问题等同于完成安全工作。再次是将攻防结果转换为治理决策的能力。学生应能够在风险控制、业务运行、处置成本和合规要求之间进行权衡，说明为什么采取封禁、隔离、降级、监测或暂缓处置等不同措施。

据此，课程体系应围绕“数据如何变成证据、攻击如何影响业务、技术判断如何形成处置决策”组织教学。每个综合项目都应同时包含模型应用、人工验证、攻防分析、业务影响判断和处置方案设计，使学生在完成任务的过程中建立三个领域之间的内在联系。

(2) 以岗位能力为主线培养网络安全实战人才

信息安全专业学生的实战培养应体现学生对复杂问题的分析能力、工程实施能力和现场责任承担能力。其培养目标应由“会操作安全工具”提升为“能够对安全任务负责”。实践教学可以按照学生承担责任的程度逐步递进。初始阶段，学生作为操作执行者，按照规范完成网络配置、漏洞验证、日志检索和系统加固；进阶阶段，学生作为问题分析者，需要从多源数据中发现线索、判断攻击过程并提出处置建议；综合阶段，学生作为任务组织者，需要协调不同角色，安排监测、分析、隔离、恢复和取证工作；岗位实践阶段，学生则应在规定权限和时间约束下，对处置结果、业务影响和技术报告承担责任。

人工智能在实践教学中应被定位为需要管理和验证的工作助手。学生可以利用人工智能完成日志归类、代码解释、告警关联和方案生成，但必须保留模型输入、模型输出、人工修改和最终判断的记录。对于封禁账户、隔离设备、修改访问策略等可能影响业务运行的操作，应要求学生完成证据确认和权限申请。这样既能提高学生使用人工智能的效率，又能防止其形成依赖模型、忽视验证的工作习惯。

(3) 发展职业本科构建产教融合实战人才培养新渠道

发展信息安全职业本科教育，是缓解复合型网络安全实战人才短缺的重要途径。相较于以理论研究为主要取向的人才培养，职业本科更加突出职业岗位、工程实践和技术应用，能够通过较长周期的项目训练，将人工智能、网络攻防和行业业务贯通起来。其产教融合不能停留在企业提供设备、讲授课程或接收学生实习，而应把校企共同解决真实安全问题作为人才培养的重要载体，使企业业务需求进入教学过程，使学生学习成果能够接受工程环境检验。

职业本科与普通应用型本科都承担应用型人才培养任务，但二者的差异主要体现在类型定位和实现机制，而非简单的层次高低。为避免把职业本科优势绝对化，具体比较见表 1。

因此，职业本科的相对优势只有在企业任务持续进入课程、教师具备工程实践能力、实训环境能够反映业务后果且评价真正依据岗位证据时才能实现。如果仍沿用知识讲授、单项实验和终结性考试，其类型优势不会自然产生。与此同时，两类本科可通过课程互选、联合项目、师资共享和应用研究形成互补。

Table 1. Comparison of talent-development mechanisms between information-security vocational undergraduate education and application-oriented undergraduate education
表 1. 信息安全职业本科与普通应用型本科的培养机制比较

比较维度	信息安全职业本科	普通应用型本科
培养逻辑	以职业岗位和典型工作任务为直接牵引，强调技术技能、工程实践与职业责任一体化	以学科专业知识应用为基础，突出理论基础、应用研究与工程实践的结合
课程组织	便于按任务簇、项目模块和工作过程组织课程，强化能力标准与评价证据对应	通常保持较完整的学科课程结构，通过实践课程和项目环节加强应用
实践载体	企业真实项目、生产性实训、岗位实践和长期项目训练占据关键位置	实验、课程设计、实习和应用研究项目是主要载体
师资协同	更强调校企双导师、产业教授和教师企业实践的常态化嵌入	以校内教师为主体，通过行业导师和校企合作补充实践指导
评价证据	侧重现场操作、工程成果、过程日志、职业规范与岗位胜任表现	兼顾课程成绩、实验项目、毕业设计及应用研究成果
适用边界	适合岗位能力边界较清晰、工程实践要求高且需快速响应技术变化的培养任务	在理论迁移、跨学科研究和较宽知识基础方面具有自身优势

4.2. 保障条件

(1) 建立以场景变化带动课程更新的机制

由于人工智能技术和攻击手段的变化速度往往快于专业建设周期。学校应保持网络基础、操作系统、程序设计、密码技术和安全原理等核心内容的相对稳定，同时建立能够快速调整的场景化教学模块。

当出现新的模型攻击、智能体风险或自动化攻防手段时，不必立即增设一门完整课程，而可以先将其转化为案例、实验或综合任务，观察其技术成熟度和岗位需求。如果相关能力逐渐成为稳定的岗位要求，再将其纳入专业核心课程。通过“先进入场景、再形成模块、最后固化为课程”的方式，既提高培养体系的响应速度，也避免课程内容因追逐技术热点而不断膨胀。

学校还应建立课程退出机制。对于已经被自动化工具替代、岗位使用频率显著降低或与真实业务脱节的训练内容，应及时压缩或调整，将教学资源投入到证据分析、复杂决策和跨领域协同等更难被工具替代的能力培养上。

场景驱动的课程模块开发可形成六步闭环：第一，持续监测岗位标准、典型安全事件、企业需求和技术趋势；第二，依据真实性、典型性、教学价值与合规风险遴选场景；第三，将场景拆解为能力目标、任务工单、数据资源、操作约束和评价证据；第四，在综合实训或项目课程中小范围试运行并保留人机协作过程记录；第五，由学生、教师和企业从能力达成、业务适用、安全合规和资源成本等方面评价；第六，根据岗位需求稳定程度决定固化为课程模块、继续迭代观察或退出。每个模块至少每学年复审一次，重大技术或合规变化发生时即时复审，具体流程见图 1。

(2) 形成以任务为纽带的跨专业教师协作机制

复合型人才不能依靠单一教师独立培养。学校应根据综合任务配置教学力量，由人工智能教师解决数据和模型问题，网络安全教师负责攻击机理和技术验证，行业人员提供业务流程和风险边界。三类人员不是分别讲授若干章节，而是共同设计同一个问题、共同观察学生的处理过程并从不同角度评价结果。教师企业实践也应由时间考核转向成果考核。专业教师进入企业后，应至少形成可以用于教学的场景、数据样本、技术任务或工程规范，并说明这些成果能够支撑哪些课程和能力目标。企业人员参与教学时，

则应避免简单介绍产品功能，而要围绕实际工作中的矛盾、失败案例和决策过程开展指导。学校在教师评价中应认可跨专业课程建设、企业问题解决、实训场景开发和技术工具研制等成果。只有当教师愿意持续进入真实业务、不同专业教师能够形成稳定合作时，复合型人才培养才不会停留在培养方案的文字表述上。

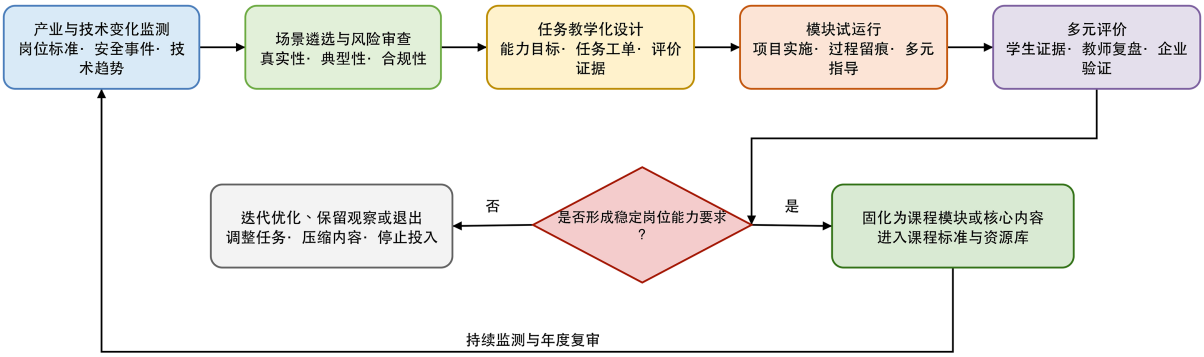

Figure 1. Scenario-driven curriculum module development process
图 1. 场景驱动的课程模块开发流程

在组织形态上，可依托项目制虚拟教研室建立跨学院、跨校企的稳定协作单元。虚拟教研室实行校企双负责人制，下设按项目组建的任务责任组，由课程负责人统筹能力目标与教学进度，人工智能教师负责数据与模型，网络安全教师负责攻击机理、验证和安全边界，企业导师负责业务流程、工程规范和成果验证。运行过程包括项目立项、场景共研、任务开发、联合授课、阶段评审、成果归档和年度复盘。线上平台用于版本管理、过程记录与资源共享，线下教研用于关键决策和实战验证，避免把虚拟教研室等同于一般资源网站或松散交流群。

配套评价应由“身份参与”转向“任务贡献”。可将评价内容划分为五类：任务与标准开发、教学资源与数据集建设、联合教学与学生指导、企业应用验证、复盘改进与成果推广。各类成果须提交可核验材料，如任务工单、评价量规、脱敏数据、课堂记录、学生作品、企业反馈和版本迭代说明。学校应把跨专业课程建设、企业问题解决、场景资源开发和技术工具研制纳入工作量及职称评价；企业成员则以场景质量、指导投入和验证反馈为主要依据。具体权重应由学校结合岗位职责另行制定，不宜在缺少制度和实测数据时设定统一比例。

(3) 建设能够反映业务后果的实战环境

传统网络靶场通常重视攻击是否成功，却较少呈现攻击对业务造成的实际后果。人工智能时代的实战环境应进一步加入业务过程和运行指标，使学生能够观察技术操作对业务服务的影响。

学校可以在隔离环境中构建业务影子系统，模拟用户登录、数据查询、交易处理、设备控制等基本业务过程，并同步配置网络流量、主机日志、安全告警和业务状态数据。学生实施扫描、封禁、隔离或恢复操作后，平台不仅反馈技术结果，还应显示服务可用性、正常用户影响、数据风险和恢复时间。这样可以促使学生将网络安全技术置于业务运行环境中理解。

(4) 建立与实战教学相匹配的安全责任制度

网络安全实战教学具有工具高危、数据敏感和操作影响范围大的特点，不能只依靠一般实验室管理制度。学校应围绕授权、数据、模型和操作建立明确的责任边界。

所有攻防任务必须有明确的测试对象、允许时间、可用工具和操作范围；所有数据必须说明来源和使用权限；使用外部大模型处理安全数据前，应判断是否涉及敏感信息外泄；对可能造成业务中断或数

据破坏的操作，应实行事前审批和过程监督。学生不仅要知道某项技术如何实施，还必须能够判断自己是否有权实施以及实施后需要承担何种责任。

教学管理可采用风险分级与责任分层相结合的制度框架。风险等级依据工具能力、数据敏感度、目标环境和业务影响综合判定，并与审批权限、监督强度和应急措施对应，具体框架见表 2。

Table 2. Risk classification and control framework for hands-on cybersecurity teaching
表 2. 网络安全实战教学风险分级与控制框架

风险层级	典型任务	审批与监督	主要控制措施
一级(低风险)	使用公开或合成数据的基础分析、隔离靶场中的常规配置与验证	任课教师审批，过程自动留痕	限定账号、环境与时间；课后复核日志
二级(中风险)	含脱敏业务数据、具备横向移动或策略变更能力的综合任务	课程负责人和实验室安全责任人联合审批，教师现场监督	数据最小化、工具白名单、快照回滚、网络隔离和双人复核
三级(高风险)	可能影响服务连续性、涉及高危工具或企业接近真实环境的任务	学院或学校授权机构审批，校企双方责任人全过程监督	书面授权、红线清单、应急中止、全量审计、成果分级和事后复盘

审批流程应包括任务申请、风险评估、授权确认、环境核验、实施监控、异常中止、结果验收和复盘归档。模型使用应记录服务提供方、输入数据类型、敏感信息处理、输出验证和人工决策；未经授权不得向外部模型提交真实漏洞细节、账号密钥、个人信息或企业敏感数据。发生越权操作、数据泄露、环境失控或业务异常时，应立即停止任务、保存证据并启动报告和处置程序。责任认定应区分制度缺陷、指导责任、操作过失和故意违规，避免以结果倒推责任。

学校应为实战教学提供持续的经费和制度支持，将平台维护、数据更新、算力使用、企业项目和教师实践纳入专业建设投入。对教师参与应急演练、企业服务和场景开发给予相应认定，防止实战教学依赖少数教师的个人投入而难以持续。

5. 讨论：实施挑战、风险与研究局限

5.1. 实施挑战及规避策略

第一，真实场景和数据具有获取难、更新快与合规要求高等特点。完全依赖企业真实项目会导致课程供给不稳定，也可能引入敏感数据和未公开漏洞。可采用“合成场景－脱敏案例－业务影子系统－授权企业项目”的分级资源体系，并建立数据来源、使用权限、保留期限和销毁方式清单。

第二，跨专业协作存在沟通成本、职责模糊和贡献难以计量等问题。项目制虚拟教研室若缺少共同任务、版本管理和成果评价，容易退化为形式化组织。规避重点是以任务书明确共同目标、角色边界、交付物和节点，以过程记录支撑工作量认定，并由校企双方定期复盘协作质量。

第三，企业参与受项目周期、商业利益和人员流动影响，长期稳定性存在不确定性。学校不宜把核心课程完全依赖单一企业，应建立多企业场景池和资源替代方案，明确知识产权、成果署名、数据安全及退出机制；对企业参与质量应以共同开发和应用验证成果评价，而非讲座次数或协议数量。

第四，业务影子系统、靶场、算力和数据更新需要持续投入，中小规模院校可能面临成本压力。可按照基础共享、专业共建和企业协同分层建设，优先保障能够直接支持核心岗位能力的场景；对使用率低、维护成本高或岗位价值下降的资源实施退出。

第五，人工智能工具快速迭代可能造成课程追逐热点、学生形成依赖以及评价真实性下降。课程更新应以稳定岗位能力而非产品版本为核心，重要任务同时提交成果件和证据件，并通过现场解释、随机变式、对照验证和人工复核确认学生真实能力。

5.2. 研究局限与后续验证

本文主要基于政策标准、相关研究和职业教育实践逻辑提出规范性框架，尚未通过多院校、长周期的实证研究检验其效果。职业本科与普通应用型本科的比较属于类型机制分析，未使用统一样本对人才培养成效作因果判断；不同学校的专业基础、区域产业、师资结构和资源条件差异，也会影响方案的可迁移性。后续研究可选择不同类型院校开展准实验或纵向追踪，以三种转化能力的量规得分、项目成果质量、现场变式表现、企业评价和毕业后岗位适应情况作为结果变量，同时考察教师协作成本、资源投入和安全事件等实施指标。在量规信度、跨评价者一致性及学生 AI 使用过程真实性得到验证前，不宜将本文框架直接作为高风险选拔或单一质量认证依据。

6. 结语

人工智能正在重塑网络攻击、防御和安全治理方式，也使网络安全能力建设中的人才制约由单纯的数量不足转变为数量短缺与能力结构失衡并存。当前真正稀缺的，不只是分别掌握人工智能、网络攻防或行业业务知识的专业人员，而是能够在复杂场景中实现跨领域贯通的人才，即能够将人工智能输出转化为可信安全证据，将技术异常转化为业务风险判断，并将攻防结果转化为可执行、可审计的治理决策。能否培养和形成这类复合型实战人才，直接影响人工智能技术能否真正转化为网络安全监测、研判、响应和处置能力。

发展信息安全职业本科教育，充分发挥其面向职业岗位、突出工程实践和深化产教融合的类型教育优势，把校企共同解决真实安全问题贯穿人才培养全过程。通过企业提供脱敏问题和业务场景、学校将其转化为教学任务、学生形成工程化成果、企业开展应用验证并反馈改进，使学生在持续完成真实任务的过程中，形成分析证据、理解业务、验证模型、权衡风险和规范处置的能力。只有建立“技术学习与业务理解相结合、AI 应用与人工验证相结合、攻防训练与责任约束相结合、学校培养与产业实践相结合”的人才培养机制，才能持续缓解复合型网络安全人才短缺，把人工智能的技术优势转化为稳定、可信、可持续的网络安全实战能力，为数字化发展和网络强国建设提供有力人才支撑。

参考文献

[1] 王磊. 人工智能时代实战型网络安全人才培养路径探究[J]. 黑龙江教育(高教研究与评估), 2026(5): 71-76.

[2] 工业和信息化部教育与考试中心, 安恒信息, 中国联合网络通信有限公司软件研究院, 等. AI 时代网络安全产业人才发展报告(2025 年) [R]. 北京: 工业和信息化部教育与考试中心, 2025.

[3] 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, 116.

[4] 人力资源社会保障部 中共中央组织部 中央网信办 国家发展改革委 教育部 科技部 工业和信息化部 财政部 国家数据局关于印发《加快数字人才培育支撑数字经济发展行动方案（2024—2026 年）》的通知[EB/OL]. 2024-04-02. https://www.gov.cn/zhengce/zhengceku/202404/content_6945920.htm, 2026-07-19.

[5] 国务院关于深入实施“人工智能+”行动的意见 国发〔2025〕11 号[EB/OL]. 2025-08-21. https://www.gov.cn/gongbao/2025/issue_12266/202509/content_7039598.html, 2026-07-19.

[6] 郭启全. “人工智能+”时代的新型网络安全实战化人才培养——以网络安全新质战斗力为引领[J]. 中国信息安全, 2026(3): 81-87.

[7] 包泽芃, 钱铁云. 大模型红队测试研究综述[J]. 计算机科学, 2025, 52(1): 7-14.

[8] 工业和信息化部人才交流中心, 工业和信息化部网络安全产业发展中心. T/MIITEC 007—2021 网络安全产业人

才岗位能力要求[S]. 2022.
https://www.miitxxzx.org.cn/module/download/downfile.jsp?classid=0&file-name=a1082cbbb71e422487b2e2c30526d7ea.pdf

[9] 陈荣丽, 杨雄, 涂娟. 人工智能时代高校网络安全教育论析[J]. 电脑与电信, 2025(3): 72-77.

[10] 李岷龙. 数智时代背景下网络安全人才胜任力模型构建[D]: [硕士学位论文]. 湘潭: 湘潭大学, 2025.

[11] European Union Agency for Cybersecurity (2019) Cybersecurity Skills Development in the EU. ENISA.

[12] 陈伟, 陈心怡. 产教融合的进化逻辑和语义解析[J]. 教育发展研究, 2025(1): 31-39.

[13] 郭文忠, 张友坤, 董晨. 网络强国战略背景下的“五位一体”信息安全人才培养模式探索[J]. 中国大学教学, 2020(10): 21-24.

[14] 苑洁, 邱朋飞, 付俊松, 等. 网络空间安全人才培养质量评价体系研究[J]. 工业和信息化教育, 2025(9): 12-16.

[15] Mulder, M. (2017) Competence-Based Vocational and Professional Education: Bridging the Worlds of Work and Education. Springer.

[16] Blumenfeld, P.C., Soloway, E., Marx, R.W., Krajcik, J.S., Guzdial, M. and Palincsar, A. (1991) Motivating Project-Based Learning: Sustaining the Doing, Supporting the Learning. *Educational Psychologist*, **26**, 369-398. https://doi.org/10.1080/00461520.1991.9653139

[17] Lave, J. and Wenger, E. (1991) Situated Learning: Legitimate Peripheral Participation. Cambridge University Press. https://doi.org/10.1017/cbo9780511815355

[18] Nonaka, I. (1994) A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, **5**, 14-37. https://doi.org/10.1287/orsc.5.1.14