

人工智能赋能高职学生网络安全教育的“三全育人” 体系构建研究

王芳

(沙洲职业工学院,江苏张家港 215600)

[摘要]随着人工智能技术的深度应用,高职学生面临的网络安全威胁呈现智能化、隐蔽化、精准化的新特征,传统网络安全教育在主体协同、过程衔接、载体覆盖和内容系统性方面面临结构性困境。本研究以“三全育人”理念为指导,结合人工智能技术特性,构建了“全员协同动态化、全程育人智能化、全域资源泛在化”的网络安全教育体系,提出了“理论模型构建—技术场景开发—政校企协同—伦理机制保障”四位一体的实施路径,旨在为高职院校培养兼具技术硬实力与伦理软素质的“数字工匠”提供系统性解决方案。

[关键词]人工智能;网络安全教育;三全育人

[中图分类号] G718.5; TP393.08

[文献标识码] A

[文章编号] 2096-711X(2026)18-0078-03

doi:10.3969/j.issn.2096-711X.2026.18.026

[本刊网址] <http://www.hbxb.net>

一、问题的提出

大数据时代的全面纵深发展深刻重塑了网络空间的安全生态。随着生成式 AI、物联网、5G 等技术的快速迭代,网络威胁呈现出智能化、隐蔽化、精准化的新特征,AI 换脸诈骗、自动化钓鱼攻击、数据挖掘隐私泄露等新型风险持续涌现。2026 年政府工作报告首次提出“打造智能经济新形态”,并强调深化拓展“人工智能+”,教育领域同样面临技术赋能与安全风险的辩证命题。高职学生作为我国数字经济发展的技能型主力军,其网络安全素养直接关系到产业数字化转型的安全根基,也关乎网络强国建设的青年人才支撑。

然而,传统网络安全教育模式在应对智能化威胁方面暴露出多重困境。从教育主体来看,网络安全教育长期被视为学生管理工作,依赖学生处、保卫处等单一部门推进,专业课教师参与度低,政府、企业、社会组织的协同育人格局尚未形成。从教育过程来看,碎片化、突击式的教育活动缺乏系统设计,往往集中在国家网络安全宣传周期间或针对大一新生开展,难以实现从知识向能力、进而向素养的螺旋式上升。从教育载体来看,传统的班团会、讲座等形式权威性不足,虚拟仿真、AI 辅助教学等数字化手段应用滞后,制约了教育实效。从教育内容来看,侧重个人防护而忽视国家网络安全战略层面的价值引领,网络安全作为国家安全重要组成部分的育人价值未能充分彰显。

教育部等九部门印发的《关于加快推进教育数字化的意见》(2026 年)明确提出“坚持数字赋能,推动教育理念、教学模式和教育治理整体性变革”,强调“促进人工智能助力教育变革”。教育部《关于深化职业教育教学关键要素改革的意见》(教职成〔2026〕1 号)进一步要求“利用大数据和人工智能精准预测关键领域人才培养供需情况”,推动职业教育人才培养由单一知识传授向综合能力提升转变。在此背景下,将人工智能技术与“三全育人”理念深度融合,构建适应高职学生特点的网络安全教育体系,既是落实国家战略部署的迫切要求,也是提升高职人才培养质量的现实命题。

二、高职学生网络安全素养的现实困境与深层成因

(一)网络安全素养的“知易行难”与群体分化

本研究通过实证调研发现,高职学生网络安全素养在认

知、技能、法律、伦理四个维度上存在显著的结构失衡。调查数据显示,网络安全意识均分 3.825(满分为 5 分),网络安全道德均分 3.920,网络安全知识均分 2.754,网络安全技能均分 2.200,呈现出“高认知、低技能、弱行为”的倒挂格局。

在安全意识层面,学生普遍存在“知易行难”的知行分离困境。96.5% 的学生认同设置安全密码的必要性,但仅有 38.9% 在实际行动中采用复杂密码设置。45.07% 的学生曾有网络账号被盗经历,41.24% 曾因个人信息泄露遭受损失。在安全技能层面,65.3% 的学生使用生日或姓名全拼设置密码,仅 28.9% 采用“字母+数字+特殊字符”组合;41.7% 的学生离开计算机时不锁定设备,34.84% 浏览陌生网站前不查看隐私政策。这些数据表明,高职学生虽具备一定的风险意识,但防护技能的转化率严重不足,面对真实安全威胁时难以将知识有效迁移到实际场景。

在网络安全道德层面,呈现出“高认同、低约束”的伦理特征。92.7% 的学生认同“不应传播网络谣言”,但 34.8% 承认曾转发未经核实的信息;41.2% 的学生认为“网络虚拟性可降低违法责任”,15.3% 曾参与网络赌博或刷单活动。更为突出的是,在具备独立编写爬虫程序能力的学生中,仅 31.8% 会主动考量隐私保护与法律法规的遵守,代码抄袭现象高达 58.6%,暴露出“技术能力与伦理责任”之间的深层失衡。

不同生源群体在网络安全素养上也呈现显著分化。农村生源学生面临“数字资源与防护需求之间的不平衡”,个人信息泄露比例高达 63.7%,显著高于城镇生源的 39.2%,但参与 CTF 等网络安全竞赛的比例极低。城镇生源学生则面临“信息过载与辨别能力不足”的困境,易受网络谣言和虚假广告影响。年级差异方面,大一学生安全意识均分最低(2.61±0.73),游戏账号交易被骗率高达 61.2%;大二学生在知识和技能维度显著提升,竞赛参与率达 34.7%;大三学生在道德与法律意识上表现最强,企业实习经历有效提升了风险应对能力。这些数据表明,高职学生网络安全素养的提升需要系统化、分层次、精准化的教育干预。

(二)网络安全教育的结构性困境

一是教学内容滞后于技术演进。当前网络安全教材的更新周期平均为 3.2 年,远远落后于网络威胁的迭代速度。

收稿日期:2026-4-24

基金项目:本文系 2025 年江苏省高校哲学社会科学研究一般项目(思政专项)“人工智能赋能高职学生网络安全教育的‘三全育人’体系构建研究”(项目编号:2025SJSZ0716)。

作者简介:王芳(1979—),女,江苏张家港人,副教授,硕士,研究方向:学生教育管理。

教学内容多集中于病毒防护、防火墙配置等传统议题,而对于AI换脸诈骗、数据画像滥用、算法歧视等大数据时代的新型威胁覆盖明显不足。师资队伍中具备企业实战经验的“双师型”教师比例仅为28%,教学内容与行业实际需求之间存在脱节。

二是数据环境加剧风险复杂性。大数据技术在带来便利的同时也催生了新型安全威胁。犯罪分子利用大数据分析构建用户画像,实施精准刷单骗局,据最新统计成功率已提升45.2%;手机App、小程序存在过度采集学生生物信息的问题,且存在未授权访问漏洞;算法推送机制形成的“信息茧房”使学生更易接触到“刷单秘籍”等不良信息,受骗风险大大增加。

三是协同育人机制尚未健全。当前高职院校网络安全教育在主体协同、过程衔接、载体覆盖和内容系统性等方面均存在短板。企业真实项目因保密要求和时间成本难以引入教学,校企合作多停留在“短期零散合作”层面,缺乏“利益共享、责任共担”的绑定机制。部分院校尚未将网络安全教育上升为“三全育人”的系统工程,而是将其视为学生管理部门的单项职责,全员、全过程、全方位的育人格局远未形成。

三、人工智能赋能“三全育人”体系的理论框架

“三全育人”即全员育人、全过程育人、全方位育人,是新时代高校思想政治工作的重要理念。2017年中共教育部党组印发《高校思想政治工作质量提升工程实施纲要》,提出推进“三全育人”综合改革,形成一体化育人制度和模式。经过多年实践,“三全育人”已形成成熟的理论框架与可操作的实践范式。将人工智能技术深度嵌入“三全育人”体系,能够从主体协同、过程优化、资源覆盖三个维度实现教育效能的重塑。

(一) 全员育人维度:从“单一主体”到“智能协同”

传统网络安全教育高度依赖学生工作部门,育人力量单一。人工智能技术可通过构建数据驱动的协同育人平台,将教师、企业导师、学生骨干、家长等多元主体纳入统一的育人网络。AI驱动的风险预警系统能够实时分析学生网络行为数据,自动生成风险等级并向不同育人主体推送干预任务——异常登录行为触发班主任预警,高危操作习惯推送辅导员介入,特定专业场景的风险由专业课教师进行精准教育,从而将“全员参与”从理念转化为可操作的协同机制。

(二) 全过程育人维度:从“节点式干预”到“全周期成长”

传统教育模式存在显著的“节点化”特征,往往集中在新生入学季或网络安全宣传周开展突击式教育,缺乏从入学到就业的全周期设计。人工智能技术通过建立学生网络安全素养的动态数字画像,能够追踪学生在认知、技能、法律、伦理四个维度上的成长轨迹,识别关键转折点,实现“入学启蒙—专业融入—实习强化—就业衔接”的阶梯式培养。基于学习行为数据的智能推荐系统,可以根据学生的年级阶段、专业类型和素养短板,推送差异化的学习资源和训练任务,使教育干预从“大水漫灌”转向“精准滴灌”。

(三) 全方位育人维度:从“课堂中心”到“全域覆盖”

传统的育人环境存在课内与课外、校内与校外、线上与线下人为割裂的状况。人工智能技术通过虚拟仿真、智能测评、跨平台数据融合等手段,能够打通不同育人场景之间的壁垒。我们可以通过虚拟攻防实训平台将课内知识与课外实践有机衔接;进一步拓展智能校园服务平台功能,将校内教育与校外服务深度融合;创新利用AI安全助手,实现正式学习与非正式学习无缝连接,从而构建起覆盖“教学—实训—生活—实习—服务”全场景的育人生态。

本研究提出人工智能赋能“三全育人”的网络安全教育理论框架,以“全员协同动态化、全程育人智能化、全域资源泛在化”为核心特征,通过“数据驱动—智能协同—场景拓展—动态评价”的四维联动机制,实现技术赋能与教育目标

的深度融合。

四、“AI+三全育人”网络安全教育体系的构建路径

(一) 全员协同:构建智能驱动的多元育人共同体

构建全员参与的网络安全育人格局,关键在于破除部门间的壁垒,整合育人力量,而人工智能技术为此种整合提供了强有力的工具保障。

其一,建立在学校党委统一领导下的网络安全教育统筹协调机制。将网络安全教育列入党委议事日程,明确各职能部门与二级学院的职责分工,形成“党委领导—部门联动—院系落实—全员参与”的工作格局。

其二,推动育人主体的数字化赋能与智能化协同。针对辅导员队伍网络安全专业知识匮乏的问题,可研发“AI网络安全教育助手”,为辅导员提供即时的专业知识支持与案例库检索服务。针对专业课教师参与度不高的问题,可在教学平台中嵌入“课程思政智能提示系统”,当专业教师讲授课程内容时,系统自动推送相关的网络安全伦理议题与教学建议,助力教师在专业课教学中融入价值引领。

其三,扩大校外育人力量的参与深度。当前部分高职院校已开展有益探索,如聊城职业技术学院联合多家网络安全服务企业,以实战化人才培养为核心,聘请企业技术总监、安全工程师担任“产业教授”,全程参与教学环节,共同设计贴合企业需求的实训课程。重庆电子科技职业大学牵头组织的网络空间安全领域高技能人才集群培养计划,强化了“行业立标、企业出题、学校答题”的协同育人理念。人工智能技术可进一步赋能这一协同过程——通过搭建“校企人才需求智能匹配平台”,将企业安全岗位能力要求转化为可量化的育人目标,将企业真实威胁情报(如本地制造业遭遇的供应链攻击案例)智能转化为课程资源,实现教育链与产业链的动态精准对接。

其四,建立多元主体的协同激励机制。可设立“网络安全素养银行”制度,将学生参与网络安全学习、竞赛、志愿服务等行为转化为可量化的积分,纳入综合素质评价;同时建立负面清单约束机制,对网络安全违规行为实施评优“一票否决”。通过正向激励与负面约束相结合,激发全员参与的主动性。

(二) 全过程贯通:打造智能化的全周期教育链条

全过程育人的核心是从入学到就业的连续性和递进性设计。人工智能技术为此提供了精准化、个性化的实现路径。

在入学阶段,通过网络安全素养基线测评,利用AI驱动的测评工具对学生进行初始画像,识别其网络安全知识储备、风险意识和行为习惯特征。针对测评结果中的薄弱环节,推送个性化学习路径——对农村生源学生定制“防刷单情景剧”,对艺术类学生推送版权法动画,对文科类学生设计信息辨伪微课,实现教育的精准化介入。

在培养阶段,构建“普及—融合—实战”三阶课程体系。面向全体学生开设《大数据安全通识》《网络安全法》等通识课程,将真实案例嵌入教学,提升教学实效。面向不同专业学生开设差异化课程——工科专业开设“工业互联网安全”与“AI安全”,文科专业增设“信息辨伪与舆情分析”,艺术类专业强化“数字版权管理”与“伦理决策”。面向学习能力突出的学生开设《CTF攻防演练》《企业红蓝对抗》等实战课程,将OWASP Top 10漏洞清单转化为实训任务。在这一过程中,AI辅助教学系统可以动态监测学生学习进度和理解程度,适时推送补充材料或挑战性任务。

在实习阶段,依托政校企协同平台,将企业真实安全项目引入教学。湖南邮电职业技术学院依托省级网络空间安全产教融合实训基地,组织学生参与全省网络安全攻防演练,两名学生入选国家“护网行动”技术团队。无锡城市职业技术学院工业互联网学院开发的“AI交互式学生智能查询助

手”,融合大语言模型、知识图谱和多模态生成技术,将传统安全教育升级为“场景化学习+智能互动+实时反馈”的闭环模式。

在就业阶段,构建“AI+岗课赛证”融通体系,通过智能算法动态匹配学生技能与企业认证标准(如华为 HCIA 安全认证),实现人才培养与岗位需求精准对接。河南经贸职业学院通过“专业+安全”融合育人实践,当年学期学生涉诈案件数量同比下降 55%,涉案金额同比下降 50%,充分验证了全过程育人的实效性。

(三)全方位覆盖:拓展全域智能的育人场景

全方位育人强调覆盖课内与课外、校内与校外、线上与线下。人工智能技术为这一全方位覆盖提供了技术支撑。

在课内课外一体化方面,打造虚实融合的沉浸式学习空间。依托虚拟仿真技术构建多模态网络攻防实训系统,模拟数据泄露应急响应、网络钓鱼识别、工业控制网络安全等真实场景。聊城职业技术学院突破传统实训模式局限,打造“师生工作室孵化+公共实训基地深化”的立体化育人载体,搭建覆盖不同学习阶段的实训平台,学生参与实训后对“企业内网攻防+合规处置”复杂任务的完成率从初期的 35% 提升至 92%。同时,部署 CyberRange 仿真平台,学生可通过 VR 设备完成“数据泄露溯源”等沉浸式任务,实现“教—学—评—战”一体化。

在校内校外协同化方面,构建“教学实战服务”的良性闭环。学校可组建“学生安全卫士”团队,鼓励学生将所学知识和技能服务社会——参与“银发数字安全助老计划”,为社区老年人安装反诈 APP 并讲解安全知识;走进中小学开展网络安全知识普及;将安全方案转化为创业项目。深圳职业技术学院学生开发的“校园 Wi-Fi 安全哨兵”系统已在 30 所院校部署,形成了“学以致用、用以促学”的良性循环。

在线上线下融合化方面,建设智能化安全教育平台。开发“风险行为诊断器”,利用 AI 技术自动分析学生网络操作行为,生成个性化防护建议。嵌入 GPT 安全助手功能,为学生提供 7×24 小时的网络安全知识问答服务。依托国家智慧教育公共服务平台,建设覆盖全学科的精品数字课程和虚拟仿真实习实践资源。无锡城市职业技术学院在“一站式”学生社区建设中,利用 AI 技术开发“应急知识图谱”功能,可智能推送个性化学习方案,实现了线上线下资源的深度融合。

(四)机制保障:构建可量化可追踪的评价与反馈系统

科学的评价体系是“三全育人”体系有效运行的关键保障。本研究构建了“网络安全素养雷达图”动态评估机制,从信息保护、法规遵守、风险识别、工具应用、隐私管理、责任担当

当六个维度建立个人素养画像。数据来源多元融合——课堂测试占 30%,行为日志占 20%,竞赛成果占 30%,企业认证占 20%,通过 AI 算法对多源数据进行整合分析,形成动态更新的学生素养档案。

在数据采集与应用过程中,必须高度重视学生数据安全与隐私保护。采用一定技术实现数据“本地处理、脱敏上传”,仅采集操作类型与响应时间等非敏感信息,明确教学数据与隐私数据的边界,确保技术赋能始终服务于育人目标而不逾越伦理底线。

评价结果的应用要形成“诊断—反馈—干预—提升”的闭环。一方面,要定期生成班级、年级、专业层面的网络安全素养分析报告,为学校决策和教育改进提供数据支撑;另一方面,要将评价结果与“安全素养银行”挂钩,防护行为转化为“安全币”,激励学生持续提升。通过数据驱动的动态评价,实现从“结果评价”向“过程评价”的转型,真正服务于学生的成长和发展。

五、结语

人工智能赋能高职学生网络安全的“三全育人”体系构建,是回应国家网络强国战略要求、落实职业教育数字化转型部署、满足高职学生全面发展需求的时代命题。本研究从“全员协同动态化、全程育人智能化、全域资源泛在化”三个维度构建了系统化的理论框架,提出了技术赋能、产教融合、伦理护航三位一体的实施路径。未来,随着生成式 AI 技术的深度整合与动态评价体系的持续优化,“数字人+自然人”双师协同育人模式将逐步普及,“技术能力+职业伦理”双驱动的育人生态亦将形成。我们唯有在技术理性与人文价值之间寻求动态平衡,才能真正为网络强国建设培养出既具备过硬技术能力又深植伦理素养的新时代“数字工匠”。

参考文献:

- [1]戴悦. 总体国家安全观视角下网络安全教育在思想政治教学中存在的问题与实施路径[N]. 安徽科技报, 2026-3-18.
- [2]教育部等九部门. 关于加快推进教育数字化的意见[Z]. 2026-2-8.
- [3]教育部. 关于深化职业教育教学关键要素改革的意见[Z]. 教职成[2026]1号, 2026-2-27.
- [4]王芳. 大数据时代高职学生网络安全素养现状调查研究[J]. 时代青年, 2025(11):111-113.
- [5]傅志平. “三全育人”在职业教育领域实施的价值意蕴及创新路径[J]. 科教文汇, 2024(7):12-18.

Research on the Construction of a “Three-wide Education” System for Cybersecurity Education of Higher Vocational College Students Empowered by Artificial Intelligence

WANG Fang

(Shazhou Institute of Technology, Zhangjiagang Jiangsu 215600, China)

Abstract: With the deep application of artificial intelligence technology, the cybersecurity threats faced by higher vocational college students have presented new characteristics such as intelligence, concealment and precision. Traditional cybersecurity education is facing structural difficulties in terms of subject collaboration, process connection, carrier coverage and content systematicity. Guided by the “three-wide education” concept and combined with the characteristics of artificial intelligence technology, this study has constructed a cybersecurity education system of “all-staff collaborative dynamicization, all-process education intelligenceization, and all-domain resource ubiquitousization”. It proposes a four-in-one implementation path of “theoretical model construction — technical scenario development — government-school-enterprise collaboration — ethical mechanism guarantee”, aiming to provide a systematic solution for vocational colleges to cultivate “digital craftsmen” with both strong technical capabilities and ethical soft qualities.

Key words: artificial intelligence; cybersecurity education; three-wide education

(责任编辑:范新菊)