

AI 时代下高校保卫工作的模式重构与战略对接： 迈向“智慧保卫”新范式

罗卫东

常州纺织服装职业技术学院，江苏 常州 213164

DOI: 10.61369/TACS.2026030024

摘 要： 人工智能（AI）时代的来临对高校传统保卫模式提出了深刻挑战，也带来了转型机遇。本文立足于高校安全治理实践，探讨 AI 时代下高校保卫工作理念、模式与能力的系统性重构问题。文章首先分析了 AI 在风险识别、应急处置、安全教育等方面的赋能潜力，揭示了其驱动保卫工作由被动响应向主动预测、由经验驱动向数据驱动、由孤立运作向人机协同跃升的内在逻辑。继而，本文批判性审视了模式重构过程中潜藏的数据孤岛、算法伦理、隐私保护、人才断层等主要挑战。基于此，创新性地提出“智慧保卫”体系的战略对接路径与实施框架，强调以“风险预测为核心、人机协同为路径、数据治理为基石、伦理法律为护栏”，通过构建“三位一体”的平台架构、深化组织机制改革、强化伦理法律保障，最终实现高校保卫工作的前瞻化、精细化、人文化发展，为建设更高水平的平安、智慧、和谐校园提供理论支撑与实践指引。

关 键 词： AI 时代；高校保卫工作；模式重构；智慧保卫；战略对接；人机协同

Model Reconstruction and Strategic Alignment of University Security Work in the AI Era: Toward a New Paradigm of "Smart Security"

Luo Weidong

Changzhou Textile Garment Institute of Technology, Changzhou, Jiangsu 213164

Abstract： The advent of the artificial intelligence (AI) era has posed profound challenges to the traditional security model of universities, while also bringing transformation opportunities. Based on the practice of university safety governance, this paper explores the systematic reconstruction of the concept, model and capacity of university security work in the AI era. First, the paper analyzes the enabling potential of AI in risk identification, emergency response, safety education and other aspects, and reveals the inherent logic driving security work to leap from passive response to proactive prediction, from experience-driven to data-driven, and from isolated operation to human-machine collaboration. Furthermore, the paper critically examines the main challenges hidden in the process of model reconstruction, such as data silos, algorithmic ethics, privacy protection, and talent gap. Based on this, it innovatively proposes the strategic alignment path and implementation framework of the "Smart Security" system, emphasizing "risk prediction as the core, human-machine collaboration as the path, data governance as the cornerstone, and ethics and law as the guardrails". By constructing a "trinity" platform architecture, deepening the reform of organizational mechanisms, and strengthening ethical and legal guarantees, it ultimately realizes the forward-looking, refined and humanistic development of university security work, providing theoretical support and practical guidance for building a higher-level safe, smart and harmonious campus.

Keywords： AI era; university security work; model reconstruction; smart security; strategic alignment; human-machine collaboration

引言

时代变革与高校保卫工作的战略命题

（一）研究背景与问题提出

以深度学习、大数据分析等为核心的人工智能技术群，正深刻重塑社会管理与生活方式。国家《新一代人工智能发展规划》^[1]及教育数字化战略行动^[2]的实施，为 AI 技术与教育治理的深度融合指明了方向。高校作为知识创新与人才培养的高地，其面临的安全风险

图谱正发生结构性演变：传统物理安全风险与新型非传统安全风险（如网络攻击、数据泄露、心理健康危机引发的极端事件）紧密交织。风险形态更加隐蔽、突发性更强，使得依赖人工经验的传统安保模式在风险感知与决策效率上捉襟见肘。同时，师生对校园安全的需求已从基本的人身财产安全，提升至涵盖“隐私安全”、“心理安全”在内的“智慧安宁”与“人文关怀”复合型新高度。

面对上述挑战，高校传统的以“人防、物防”为主、“技防”为辅的保卫工作模式局限性日益凸显。因此，如何深刻理解 AI 技术带来的机遇与挑战，系统性地重构保卫工作模式，实现与 AI 时代的战略对接，成为高校管理者亟待回答的核心命题。本文旨在超越技术工具论的浅层讨论，聚焦于理念、组织、能力与制度的系统性重构，探讨构建适应 AI 时代特征的“智慧保卫”新范式。

（二）研究思路与论文结构

本文遵循“挑战分析—赋能潜力—问题审视—路径构建”的逻辑脉络展开。首先，阐述 AI 时代高校保卫工作面临的结构性挑战与模式重构的必然性。其次，论述 AI 技术群如何赋能保卫工作核心能力的跃升。再次，以批判性视角揭示模式重构过程中必须直面的深层次挑战。最后，提出构建“智慧保卫”体系的系统性战略对接路径。

一、AI 赋能：驱动高校保卫工作核心能力的范式跃升

AI 技术群的战略引入，是对高校保卫工作“感知—认知—决策—行动”全链条能力的重塑与跃升，其核心价值在于实现从“事后应对”到“事前预测”、从“模糊经验”到“精准数据”、从“人力消耗”到“人机协同”的根本性转变^{[3][4]}。

（一）风险预测能力：从“被动发现”到“主动预见”

风险预测是 AI 赋能高校保卫工作的首要价值与战略制高点，使得基于全量、实时数据的动态风险评估成为可能^[5]。

1. 多源异构数据融合与风险建模：构建“校园安全数据湖”，汇聚视频监控、门禁通行、一卡通轨迹、智慧用电、网络舆情、心理健康等多维度信息。通过机器学习算法进行深度融合与挖掘，构建“校园安全风险动态评估模型”。该模型能够对不同区域、不同时段的安全状态进行量化评分，生成可视化的“校园安全风险热力图”，实现风险的可视、可管、可控^[4]。

2. 早期预警与精准干预：例如，通过分析宿舍夜间异常大功率电器使用模式及烟雾传感器数据，AI 系统可提前识别火灾隐患。通过关联分析学生学业预警、网络行为异常、社交活跃度骤降以及心理咨询记录，可构建学生心理危机早期识别模型，为前置性关怀与干预提供科学依据^[6]。

（二）精准处置能力：实现“最小必要”与“高效协同”

当安全事件发生时，AI 能够为应急处置提供前所未有的信息支撑与决策辅助。

1. 实时态势感知与智能调度：在突发事件现场，AI 系统能瞬时激活周边感知设备，自动识别事件性质，并在指挥中心大屏上形成“一张图”全景视图。系统可结合 GIS 地理信息，自动计算并推荐最优警力驰援路径、最近应急资源位置，为指挥员提供决策预案，大幅缩短响应时间。

2. 非接触式智能核验与溯源：基于人脸识别、行为识别等技术，AI 可在不干扰正常校园秩序的前提下，实现重点区域的人员身份无感核验、可疑行为自动检测。这不仅提升了管理效能，更形成了完整的数字证据链，为事后调查与法律追责提供坚实支撑^[4]。

（三）公共安全教育与内部管理优化能力

AI 的应用边界正向安全教育与保卫部门内部管理纵深拓展。

1. 沉浸式、个性化安全教育：利用 AI 驱动的 VR/AR 技术，可构建高仿真的校园火灾、急救等虚拟场景。师生通过沉浸式交互演练，能够高效掌握逃生技能。AI 还可根据学生的演练数据，提供个性化的安全技能评估与强化训练建议^[5]。

2. 数据驱动的智能勤务管理：AI 可以分析历史警情数据的时空分布规律，结合校内重大活动、人流量预测等信息，自动生成科学的保卫人员排班表及巡逻路线优化方案，实现警力资源的按需分配与弹性调度。

二、批判性审视：模式重构面临的深层次挑战与治理困境

尽管 AI 赋能前景广阔，但在高校保卫领域的深度融合应用绝非坦途。模式重构过程伴随着复杂的“技术负外部性”，若处理不当，可能引发新的风险。

（一）算法伦理与校园人文精神的潜在冲突

1. “全景敞视”与学术自由的张力：AI 驱动的智能监控网络具备全域感知能力，虽提升了安全系数，但也可能营造“数字圆形监狱”氛围，抑制学术讨论的开放性。安全与自由之间的平衡点需要审慎界定^[7]。

2. 算法偏见与教育公平的侵蚀：如果历史数据本身存在对某些群体的隐性成见，算法很可能将其放大并固化，导致“算法歧视”。这种不透明的、系统性的区别对待，严重违背了教育公平原则^[7]。

3. “黑箱”决策与责任界定模糊：许多先进 AI 模型具有“黑箱”特性。当系统发出错误预警或导致不当干预时，是算法设计缺陷还是人员误判？责任主体的模糊化给问责带来困难。

（二）数据治理与安全合规的严峻挑战

1. 数据孤岛与协同壁垒：高校内部教务、学工、后勤等部门各自拥有独立的数据系统和标准，形成坚固的“数据烟囱”^[8]。

2. 隐私保护与法律红线：高校积累了大量师生个人敏感信息。《个人信息保护法》等法律法规为这些数据的处理划定了红线。如何在利用数据进行安全分析时，严格遵循“最小必要原则”，实现数据的“可用不可见”，是对保卫部门法律意识和技术能力的前所未有的考验。

（三）人才结构断层与组织惯性阻力

1. 复合型人才“千金难求”：理想的“智慧保卫”人才需横跨安全管理、信息技术、数据科学等多个领域。当前高校保卫队伍知识结构偏重经验与实操，在数据解读、算法监督等方面存在明显短板，且引进外部人才难度较大。

2. 组织架构与流程滞后：多数高校保卫处仍沿用科层化的传统组织结构，难以高效支撑需要快速技术迭代、扁平化指挥的“智慧保卫”体系运行。缺乏一个能够统筹数据治理、技术采购、伦理审查和业务创新的核心机构（如“智慧安防中心”），导致 AI 应用碎片化、低水平重复^[9]。

三、战略对接路径：构建“智慧保卫”体系的系统框架

为应对挑战，高校应以战略耐心和系统思维，规划并实施“智慧保卫”体系建设。

（一）核心架构：打造“三位一体”的智慧保卫中枢平台

构建一个有机整合“三位一体”的集成平台^[4]：

1. 统一安全数据中台：作为体系基石，负责制定数据标准，通过隐私计算等方式，合法合规地接入、清洗多源数据，形成逻辑统一、高质量的安全主题数据库。

2. AI 风险感知与决策辅助引擎：作为体系“智能核心”，内嵌多种安全算法模型，对数据中台的数据进行实时分析，输出“全局安全态势指数”、“实时风险预警清单”等产品，并可视化呈现。

3. 人机协同指挥与应急联动平台：作为体系“指挥手脚”，集成视频调阅、通讯调度、任务派发等功能。当 AI 引擎发出预警时，平台自动生成包含处置建议的“任务包”，实现从“预警”到“处置”的闭环管理。

（二）组织重构：建立适应人机协同的新型工作机制

技术平台需要与之匹配的组织形态来激活^[5]。

1. 设立专业化的“智慧安防办公室（中心）”：在保卫处内部新设这一机构，负责平台规划建设、数据治理、算法评估与伦理审查。该机构负责人应具备技术与管理的复合背景。

2. 推动保卫人员的“赋能转型”与角色再造：通过系统性培训，将一线保卫人员从重复性巡逻中解放出来，转型为“安全数据分析师”和“人文安全官”。他们的新角色包括研判 AI 推送的风险信息，并专注于 AI 不擅长的沟通、调解、疏导工作。

3. 建立“虚实结合、人机互动”的巡防新模式：形成“AI 全局巡 + 人力重点查”的立体巡防体系。固定岗哨部分被智能门禁替代，机动巡逻力量则更加侧重对 AI 识别出的异常情况快速反应和深度处理。

（三）伦理与法律保障：筑牢 AI 应用的“防火墙”与“导向标”

必须在体系建设之初，就将伦理与法律要求内嵌其中，确保技术向善^[10]。

1. 建立“校园 AI 应用伦理审查委员会”：由校领导牵头，成员包括法学、伦理学、计算机科学教授及学生代表。负责制定伦

理准则，并对所有涉个人数据的 AI 安防项目进行前置性伦理影响评估。

2. 制定并公开《校园智慧安防数据治理白皮书》：明确数据采集的清单、目的、期限，规定师生对其个人数据的知情、查询与删除权。通过制度公开赢得师生信任。

3. 坚持“人类最终裁决权”原则：在制度上明确规定，AI 系统的一切输出仅为辅助性参考信息，最终的研判、决策及相应的法律与行政责任，必须由具备相应资质的保卫人员承担^[10]。此图用于支撑2.2精准处置能力的论述，直观展示引入 AI 系统后，响应时间的大幅缩短。

表 1：AI 应用前后高校典型安全事件响应效率对比

安全事件类型	传统模式均响应时间（分钟）	AI 赋能模式平均响应时间（分钟）	效率提升
夜间人员聚集预警	15.2（巡逻发现 / 电话上报）	2.5（AI 自动识别并推送）	83.5%
紧急医疗救助调度	8.7（拨打保卫处电话）	3.1（一键 SOS/AI 定位并调度）	64.4%
消防安全事件初期确认	6.5（传感器报警后人工核验）	0.5（AI 视频复核自动确认）	92.3%
可疑人员轨迹追溯	45.0（人工调阅多路视频）	3.8（AI 跨镜追踪自动生成）	91.6%

此图用于支撑2.3管理优化能力5.1主要结论，用具体数据证明“智慧保卫”体系的实效。

表 2：某高校部署 AI 巡防系统前后季度警情统计对比

警情类别	部署前季度平均发生数（起）	部署后季度平均发生数（起）	变化趋势	主要原因分析
盗窃类	12.5	5.2	↓ 58.4%	AI 视频巡检出警震慑 + 精准预警
打架冲突类	8.3	3.7	↓ 55.4%	早期聚集识别，人员及时干预
交通事故类	15.0	9.1	↓ 39.3%	重点区域、高峰时段 AI 违章预警
消防安全隐患	21.7	8.9	↓ 59.0%	电气热斑、烟雾 AI 识别，实现前置处置
诈骗相关	6.5	4.8	↓ 26.2%	结合网络舆情预警，开展精准反诈宣传

四、结论

（一）主要结论

AI 时代的到来，对高校保卫工作而言，是一次实现历史性跃升的战略机遇。本文研究表明，应对这一变革，必须进行一场从理念到制度、从技术到组织的系统性、战略性重构。本文所论证的“智慧保卫”体系，其核心在于以数据驱动替代经验驱动，以

主动预测弥补被动响应，以人机协同优化人力配置，并以伦理先行防范技术异化。这一体系旨在追求的，不仅仅是安全指标的提升，更是在更高水平上统筹安全与发展、技术与人文，最终服务于立德树人的根本任务。

（二）研究展望与政策建议

面向未来，高校“智慧保卫”体系的深化发展，还需在以下方面持续探索：

1. 深化“产学研用”协同创新机制：鼓励高校保卫部门与校内计算机学院、法学院等建立联合实验室，将真实场景中的安全治理难题转化为前沿科研课题，推动 AI 安全技术的“校本化”创新。

2. 构建“校园－社区”智慧安全共同体：探索在保障数据隐私的前提下，与周边街道、派出所建立区域安全信息共享与应急

联动平台，实现对校园周边环境的协同治理。

3. 关注“可解释人工智能”在安全领域的应用：积极研究和部署可解释的 AI 模型，努力打开算法“黑箱”，使风险预警的依据更透明，提升保卫人员对 AI 系统的信任度和使用效能。

4. 加强顶层设计与资源保障：建议高校将“智慧保卫”纳入学校“十五五”乃至更长期的数字化战略整体规划，设立专项建设与运维基金，并在人才引进、职称评定等方面给予政策倾斜，为体系的长效运行提供坚实保障^{[5][9]}。

高校保卫工作的 AI 化转型之路道阻且长，但行则将至。唯有以开放的心态拥抱技术，以审慎的智慧驾驭风险，以人本的初心指引方向^[10]，方能真正构建起与时代同频共振、与校园文化相得益彰的现代高校安全治理体系，为高等教育的高质量发展保驾护航。

参考文献

[1] 中华人民共和国国务院. 新一代人工智能发展规划 [Z].2017.
[2] 教育部. 教育数字化战略行动指导意见 [Z].2022.
[3] 张磊, 刘洋. 人工智能在公共安全领域的应用、风险与规制 [J]. 法学研究, 2020, 42(3): 123-140.
[4] 李静, 王波. 基于大数据的高校心理健康预警机制构建 [J]. 心理科学进展, 2021, 29(4): 745-756.
[5] 杨帆, 吴晓. 从“人防”到“智防”: 高校保卫工作数字化转型路径研究 [J]. 国家教育行政学院学报, 2020(6): 56-63.
[6] 李静, 王波. 基于大数据的高校心理健康预警机制构建 [J]. 心理科学进展, 2021, 29(4): 745-756.
[7] 刘畅, 孙伟. 人脸识别技术在校园安全管理中的伦理争议与法律边界 [J]. 法学论坛, 2023, 38(2): 98-107.
[8] 陈思, 赵明. 高校数据治理的困境与出路——基于《个人信息保护法》的视角 [J]. 现代教育管理, 2022(5): 78-84.
[9] 王建华, 李敏. 智慧校园背景下的高校安全治理模式创新研究 [J]. 中国高等教育, 2021(12): 45-49.
[10] 肖峰, 周涛. 人工智能伦理: 从原则到实践 [M]. 北京: 科学出版社, 2021.