Computer Science and Application 计算机科学与应用, 2026, 16(6), 232-241
Published Online June 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.166223

Hans汉斯

数智化时代高校网络安全“全域协同”治理体系的重构与制度化实践

周　敏，陈伟杰*，陈泽生，冯李春，李炳南，陈勇标

广州美术学院信息技术中心，广东 广州

收稿日期：2026年5月15日；录用日期：2026年6月19日；发布日期：2026年6月29日

摘　要

在人工智能、大数据等颠覆性技术集群式突破的数智化时代，高等教育正经历从规模供给向智能化提质增效的深刻转型。网络安全作为数字化底座的生命线，其治理逻辑已从传统的碎片化防御转向全域协同的系统重构。本文立足于2026年全球网络安全格局及“十五五”规划背景，结合广州美术学院等高校的制度化实践，系统阐述了高校网络安全“全域协同”治理体系的理论内涵、重构逻辑与实践路径。研究发现，通过“技术–制度–价值”三层融合治理模型，确立“谁主管谁负责、一数一源、全生命周期管控”等制度化规范，能够有效应对AI驱动的自动化攻击与深伪技术等新型威胁。本文旨在为教育信息化网络安全管理体系的深化改革提供理论支撑与实务指引。

关键词

数智化时代，高校网络安全，全域协同，制度建设

Reconstruction and Institutionalized Practice of a “Comprehensive Collaboration” Governance System for Higher Education Cybersecurity in the Digital Intelligence Era

Min Zhou, Weijie Chen*, Zesheng Chen, Lichun Feng, Bingnan Li, Yongbiao Chen

Information and Technology Center, Guangzhou Academy of Fine Arts, Guangzhou Guangdong

Received: May 15, 2026; accepted: June 19, 2026; published: June 29, 2026

*通讯作者。

文章引用: 周敏, 陈伟杰, 陈泽生, 冯李春, 李炳南, 陈勇标. 数智化时代高校网络安全“全域协同”治理体系的重构与制度化实践[J]. 计算机科学与应用, 2026, 16(6): 232-241. DOI: 10.12677/csa.2026.166223

Abstract

In the digital intelligence era marked by clustered breakthroughs in disruptive technologies such as AI and big data, higher education is undergoing a profound transformation from scale-driven supply to intelligent quality improvement and efficiency enhancement. As the lifeline of the digital infrastructure, cybersecurity governance has shifted from traditional fragmented defense to a systemic reconstruction of comprehensive collaboration. Based on the global cybersecurity landscape in 2026 and the context of the 15th Five-Year Plan, this paper systematically elaborates on the theoretical connotation, reconstruction logic, and practical pathways of the "comprehensive collaboration" governance system for university cybersecurity, drawing on institutionalized practices from institutions like the Guangzhou Academy of Fine Arts. Research findings reveal that through a three-tiered integrated governance model of "technology-institution-value," establishing institutionalized norms such as "whoever oversees bears responsibility, one source for each dataset, and lifecycle management" can effectively counter new threats like AI-driven automated attacks and deepfake technologies. This study aims to provide theoretical support and practical guidance for the deepening reform of cybersecurity management systems in educational informatization.

Keywords

Digital Intelligence Era, Higher Education Cybersecurity, Comprehensive Collaboration, Institution Building

1. 引言

在“十五五”规划开局起步、教育强国建设进入纵深推进的关键阶段，以人工智能、大数据、大模型为核心的数智化技术，正推动高等教育领域发生从“数字化叠加”到“数智化重构”的根本性范式跃迁。数智化转型绝非技术工具在教育场景的简单应用，而是以数据为核心生产要素、以智能算法为核心驱动力，对人才培养、科研创新、校园治理和社会服务全链条进行的系统性重塑。近年来，我国持续实施教育数字化战略行动，智慧校园、在线教育平台、科研大数据协同体系、AI 辅助教学与管理系统已成为高校办学的基础配置，数智化已成为新时代高等教育高质量发展的核心引擎与鲜明标识。

然而，数智化在全面释放高等教育生产力的同时，也彻底打破了传统校园的物理边界与网络安全防护逻辑，使网络空间成为高校风险防控的核心主阵地。与数字化时代相比，数智化时代的高校网络环境呈现出虚实深度融合、接入节点泛在化、数据要素高流动性、算法应用全场景渗透的核心特征，与之相伴的是网络安全威胁的代际升级。其中，AI 发起的自主化、规模化攻击，深伪技术驱动的高精准社会工程学诈骗，量子计算发展对现有加密体系的潜在冲击，以及大规模师生个人信息与科研敏感数据泄露风险，共同构成了高校网络安全面临的跨代威胁。

作为开放度高、流动性强、数据密集型的特殊网络空间主体，高校的网络安全治理有着区别于政府机关、企业主体的独特性与复杂性：高校既是国家关键信息基础设施的重要组成部分，承载着基础学科研究、关键核心技术攻关的敏感科研数据；也是面向数十万师生的公共服务主体，掌握着海量个人敏感信息；同时还是网络意识形态建设与青年网络素养培育的核心阵地，其网络安全直接关系社会的安全稳

定[1]。面对全新的威胁形态，我国高校传统的网络安全治理模式逐渐显现出深层困境：以物理边界为核心的“单点防护”思维难以应对泛在化的接入风险，多部门分散管理的“碎片化防御”体系难以形成治理合力，重技术建设、轻制度落地、轻价值引领的治理惯性，无法适配数智化时代全流程、全要素、全主体的安全治理需求。在此背景下，如何突破传统治理范式的局限，重构一套适配数智化时代特征的高校网络安全治理体系，已成为当前我国高等教育数智化转型中亟待破解的核心命题。

从现有研究来看，学界围绕高校网络安全治理已形成一批成果，多集中于技术防护体系优化、单一制度规范建设、特定风险场景应对等维度，为相关实践提供了基础支撑。但现有研究仍存在明显的拓展空间：朱晓飞等人[2]结合自适应安全框架 3.0 和信息系统建设“分层解耦、异构兼容”的理念提出了一套自适应实战化安全运营体系建设方案，但其停留在智慧校园的背景下，缺乏对数智化时代 AI 驱动的新型威胁的系统性回应。顾坤坤等人[3]以 DSG、DSMM 数据安全治理思路为指导，构建了高校数据安全治理的思路和治理框架，林智钦等人[4]通过加强安全技术防护和加强与外部安全维护团队的合作等措施提升了高校机房网络安全管理水平，王淑荣等人[5]从内涵界定、风险根源和传播机理等角度对数智时代高校网络意识形态进行风险研判并提出相应对策，但上述研究未从体系化视角构建高校网络安全治理的整合性理论框架，对技术、制度、价值多维度融合的治理逻辑探讨不足，同时缺乏结合高校具体制度化实践的实证分析。

基于此，本文以数智化时代高校网络安全治理的范式转型为核心研究对象，构建“技术－制度－价值”三层融合的治理逻辑框架，界定高校网络安全“全域协同”治理的核心内涵与转型要求。同时，本文以广州美术学院 2026 年系列网络安全管理制度建设与实践为实证样本，系统梳理高校网络安全“全域协同”治理的制度化实践路径，最终提出数智化时代高校网络安全治理体系的深化建设建议。本文的研究，既旨在丰富高校网络安全治理的理论体系，也为我国高校在“十五五”时期应对数智化安全挑战、筑牢教育强国建设的安全屏障，提供可复制、可推广的实践参考。

2. 高校网络安全治理的逻辑重构

数智化技术对高等教育生态的系统性重构，不仅带来了网络安全威胁形态的代际升级，更从根本上动摇了传统高校网络安全治理的底层逻辑。面对 AI 驱动的“跨代威胁”与泛在化的安全风险，高校网络安全治理必须完成从“单点防御”到“全域协同”的范式转型，构建“技术－制度－价值”三层融合的治理框架，为治理体系的重构与制度化实践提供核心理论支撑。

2.1. 治理范式的转型：从“单点防御”到“全域协同”

传统高校网络安全“单点防御”范式，以物理网络边界为核心、技术设备堆砌为手段、网信部门单一主体主导，适配了数字化初期封闭静态的校园网络环境。但数智化时代，高等教育生态虚实融合、接入节点泛在、数据高流动、算法全场景渗透的特征，让该范式局限性全面凸显，一是固定边界防护逻辑失效，泛在接入终端、跨场景应用与校外云服务彻底打破校园物理边界；二是碎片化管理形成治理盲区，网络安全被视为网信部门专属职责，二级单位主体责任缺失“双非”系统、私建网络等成为防控真空；三是被动响应模式严重滞后，重事后处置、轻事前预防的传统逻辑，无法应对 AI 自动化攻击、深伪诈骗等瞬时性新型风险。

数智化时代高校网络安全治理的核心转型方向，是从“单点防御”向“全域协同”范式的系统性跃迁。该范式以保障高等教育数智化转型为目标，以系统治理思维打破各类壁垒，构建全主体、全要素、全流程的系统性治理模式，核心转型逻辑分为三个维度：一是治理主体从“单一主导”向“全员协同”转型，以“党管网信”为核心，形成全主体责任闭环；二是治理范围从“边界防护”向“全场景纳管”转

型，覆盖校园全场景网络空间要素，消除治理盲区；三是治理模式从“被动响应”向“全流程主动防控”转型，构建全流程治理闭环，推动治理从经验驱动向数据驱动、被动补救向主动防控的根本转型。

2.2. 理论框架：技术－制度－价值的三层融合模型

“全域协同”治理体系的构建，不能局限于技术升级或制度堆叠，必须建立技术、制度、价值三层深度融合的治理逻辑，如图 1 所示。形成“技术为底座、制度为骨架、价值为灵魂”的整合性理论框架，破解高校网络安全治理中“技术与制度脱节、管控与价值背离”的核心痛点。

Figure 1. “Technology-Institution-Value” three-layer integration model for higher education cyber-security governance
图 1. 高校网络安全治理“技术－制度－价值”三层融合模型

2.2.1. 技术层：智能感知与主动防控的治理底座

技术层是“全域协同”治理的底层支撑，核心功能是通过数智化技术构建主动防御体系，推动防护模式从“被动响应”向“主动防控”转型，解决 “能不能防”的核心问题。

数智化时代网络攻防已进入“AI 对抗 AI”新阶段，传统基于规则的防护技术难以适配 AI 自动化攻击、深伪诈骗等新型威胁。技术层核心建设逻辑，是依托大数据、AI、态势感知等技术，构建全网实时监测体系，重点打造全资产可视化、智能威胁识别、数据安全防护、快速应急响应四大核心能力，实现风险早发现、早预警、早处置。

2.2.2. 制度层：协同机制与权责闭环的治理骨架

制度层是“全域协同”治理的核心骨架，核心功能是通过系统化制度设计，明确权责、规范流程、建立协同机制，监督管理技术运行与治理行为，解决“能不能管”的核心问题。

制度层建设遵循“于法有据、贴合实际、全域覆盖、闭环管理”原则，核心构建四大制度体系。一是全级责任制度，以“党管网信”为核心，通过责任书实现责任全级传导，形成权责闭环；二是全场景管理制度，覆盖校园网络、数据安全、软件资产等全场景，消除监管盲区；三是全流程管控机制，建立事前预防、事中管控、事后处置的全流程规范；四是合规适配机制，全面对标国家网络安全相关法律法规，确保校内制度合规落地。

2.2.3. 价值层：价值引领与内生自觉的治理灵魂

价值层是“全域协同”治理的内核灵魂，核心功能是通过价值引领强化师生主体地位，推动治理约束从外部合规转化为全员内生自觉，解决“愿不愿守”的核心问题。

高校网络安全治理的根本目标，是为高等教育数智化转型筑牢安全屏障，落实立德树人根本任务。价值层建设核心是破解“重管控、轻服务”“重合规、轻育人”的误区，实现三大价值引领，一是坚守教育本质，推动安全治理与办学核心职能深度融合，实现安全与发展的动态平衡；二是保障师生权益，遵循个人信息保护核心原则，通过常态化安全教育，将师生从防控薄弱环节转化为治理核心主体；三是筑牢意识形态阵地，强化信息内容管控，引导师生树立正确的网络安全观与法治观念。

2.2.4. 三层融合的内在逻辑

技术层、制度层、价值层并非孤立模块，而是深度融合、相互支撑的有机整体。技术层为制度落地提供技术支撑，制度层监督技术应用，价值层为技术与制度建设指明根本方向。三者的深度融合，共同构成了高校网络安全“全域协同”治理体系的完整理论逻辑，为治理体系重构与制度化实践提供了系统性理论框架。

3. “全域协同”治理体系的制度化实践探索

数智化时代高校网络安全“全域协同”治理体系的落地，核心是将理论框架转化为系统化、可执行的制度化实践。如图 2 所示，广州美术学院以应对数智化新型安全威胁为导向，于 2026 年集中修订印发网络与信息安全管理办法、校园网络管理办法、软件正版化管理办法、个人信息保护管理办法、数据安全管理办法、校园邮件管理办法等系列制度文件，构建起覆盖组织、资产、数据、应用全维度的“全域协同”治理制度体系，形成了可复制、可推广的高校网络安全治理实践范式。

3.1. 组织架构协同：构建“党管网信”统领的全级责任闭环

组织架构协同是“全域协同”治理的核心前提，核心目标是打破网信部门“单打独斗”的碎片化格局，构建权责清晰、协同联动的全主体治理架构。

学校以制度化形式确立“党管网信”顶层架构，明确网络安全与信息化工作领导小组为最高领导机构，由学校党委书记任组长，统筹网络安全重大事项决策与部署。在此基础上，构建“领导小组－工作小组－技术支撑部门－业务主管部门－二级单位”五级协同治理架构，清晰划定各主体权责边界，二级单位同步成立网信工作小组，明确党政负责人为第一责任人，实现治理主体横向到边、纵向到底。

同时，学校以“谁主管谁负责、谁运维谁负责、谁使用谁负责”为核心原则，通过全员签署《网络与信息安全责任书》实现责任全级传导，建立人员变更实时补签机制，并设置全梯度追责问责体系，形成“责任明确－传导到位－监督有力－追责闭环”的全级责任体系，为全域协同治理提供坚实组织保障。

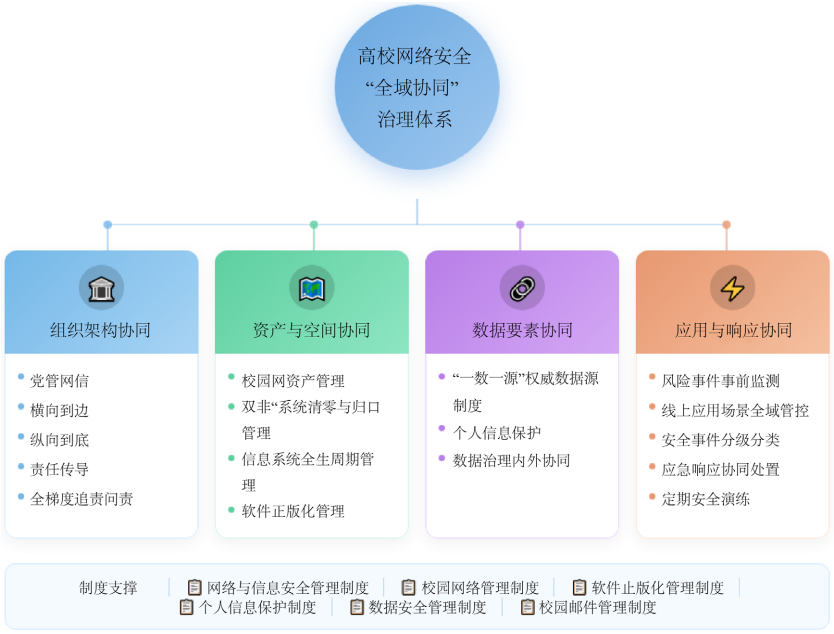

Figure 2. “Comprehensive collaborative” governance system for higher education cybersecurity
图 2. 高校网络安全“全域协同”治理体系

3.2. 资产与空间协同：实现全要素网络资产的无盲区纳管

资产与空间协同是“全域协同”治理的基础支撑，核心目标是打破传统治理的监管盲区，实现校园网络空间资产的全要素、全周期纳管。

学校以制度明确校园网络空间是学校管理权的自然延伸，校园网所有硬件设备、网络系统、配套设施、IP 地址、域名等资产均为学校公共资产，由信息技术中心统一规划管理，严禁私建网络、私拉线缆、私自占用网络资源，从源头杜绝私建网络带来的安全隐患。针对高校普遍存在的“双非”系统监管难题，建立清零与归口管理制度，明确此类系统原则上关停，确需运行的须迁移至校内统一平台并完成合规备案；同时建立信息系统全生命周期管理制度，落实“三同步”原则、上线安全测评、校外开放白名单、涉密系统物理隔离、废弃系统注销备案等要求，实现全流程闭环管理。

此外，学校将软件正版化纳入全域治理体系，通过专项管理办法明确各级责任主体，规范正版软件采购、授权、使用、监督全流程，防范盗版软件带来的安全漏洞与知识产权风险，补齐了资产治理的传统短板。

3.3. 数据要素协同：建立全生命周期的数据安全与个人信息保护体系

数据要素协同是“全域协同”治理的核心内核，核心目标是破解数据治理乱象，实现数据要素全生命周期协同治理，守住数智化转型的数据安全底线。

学校以制度化形式确立“一数一源”权威数据源制度，明确人事、教务、研究生系统分别为教职工、本科生、研究生信息的唯一权威数据源，其他部门不得重复采集个人信息，从根源上解决“数据烟囱”、“多点采集”等问题。针对个人信息保护核心痛点，通过专项管理办法明确个人信息与敏感信息范围，确立“合法正当、最小化、公开透明”等核心处理原则，对个人信息采集、存储、使用、共享、公开、删除全环节作出刚性规范，同时明确师生信息查询、更正、举报等合法权益，兼顾数据治理与权益保护。

此外，学校建立数据治理内外协同机制，要求与第三方服务商合作必须签署安全保密协议，明确数

据安全责任与违约责任；同时建立违规行为处置与追责机制，实现数据安全治理的内外协同与闭环管控。

3.4. 应用与响应协同：构建适配新型威胁的全流程闭环管控体系

应用与响应协同是“全域协同”治理的关键抓手，核心目标是破解传统治理“重建设、轻运维”、“重防护、轻响应”的痛点，针对数智化新型瞬时风险构建全流程闭环管控体系。

针对高频风险应用场景，学校建立常态化协同管控制度。通过《校园邮件管理办法》规范邮件系统统一建设与归口管理，落实实名制、僵尸账号定期清查、违规账号禁用注销等要求，防范钓鱼诈骗风险；同时规范新媒体账号、LED 显示屏、交互类栏目等场景管理，明确新媒体账号备案审批、信息发布审核、交互栏目实名制等要求，实现线上应用场景全域管控。

针对新型攻击的瞬时性特征，学校建立分级分类、高效协同的应急响应机制，将网络安全事件划分为六大类、四个等级，明确不同等级事件的处置主体与响应时限，要求 I 级、II 级事件 3 分钟内采取紧急处置措施、15 分钟内完成上报；同时要求各单位制定专项应急预案、定期开展演练，建立“监测－通报－整改－复核”的动态管控闭环，实现安全风险的前置防控与全流程闭环处置。

4. 高校网络安全“全域协同”治理体系的深化路径与优化建议

数智化技术的持续迭代与高等教育数字化转型的纵深推进，决定了高校网络安全治理是一个动态优化、持续完善的长期过程。前文构建的“技术－制度－价值”三层融合理论框架与广州美术学院的制度化实践，为高校网络安全从“单点防御”向“全域协同”转型提供了核心逻辑与实践样本。面向“十五五”时期教育强国建设的核心目标，应对 AI 攻防升级、数据安全风险加剧、跨境网络威胁蔓延等全新挑战，高校需在现有实践基础上，从技术底座、制度闭环、数据治理、主体生态、国家站位五个维度，持续深化“全域协同”治理体系建设，全面提升高校网络安全治理的系统性、主动性与韧性，为高等教育数智化转型筑牢安全屏障。

4.1. 强化技术底座升级，构建人机协同的全域智能主动防御体系

技术层是“全域协同”治理体系的底层支撑。潘柱廷[6]提出网络安全攻防博弈已通过 AI 能力提升迈向高维智能化阶段，AI 与安全得到了进一步的融合发展。高校需突破传统“设备堆砌、被动补救”的建设逻辑，以“AI 对抗 AI”为核心，构建全域覆盖、智能感知、主动预警、快速响应的人机协同智能防御体系，实现技术防护能力的代际升级。

第一，建设 AI 驱动的全域网络安全态势感知平台。在网络安全领域，大语言模型已经用于漏洞识别、入侵检测、恶意软件研究、网络攻击识别和钓鱼邮件识别等任务[7]，因此可在学校现有安全监测能力基础上，整合校园全维度数据，依托大语言模型与相应算法构建攻击识别模型，实现新型威胁的实时监测与智能预警；打通校内相关部门的数据壁垒，实现威胁情报共享与协同研判，形成“全网一张图、监测无死角”的防控格局。

第二，构建全生命周期的资产与终端安全管控体系。通过自动化资产识别与梳理，实现校园全网络资产的动态盘点与可视化管理，从根源上消除各类资产安全盲区；推广终端安全管理系统，实现补丁更新、病毒防护、违规监测的集中管控，补齐终端防护短板。

第三，建立常态化攻防演练与主动防御机制。当前电信网络诈骗屡屡发生，呈现出产业化、集群化特征[8]，高校师生普遍网络安全意识较为薄弱，极易成为犯罪分子的目标。为提升师生主动防御能力和安全意识，定期开展实战化攻防演练与反诈实训；联合第三方安全机构建立常态化红蓝对抗机制，开展渗透测试与漏洞挖掘，推动技术防护从事后补救向事前预防、主动防控转型。

第四，推进自主可控的信创技术体系适配。加快校园信息系统的信创适配改造，优先完成基础硬件和操作系统的替换升级，再逐步推进数据库、中间件、应用软件等各层级的适配改造[9]，优先选用自主可控的技术产品，防范底层供应链安全风险，构建自主、安全、可控的技术底座。

4.2. 完善制度闭环建设，推动全域协同治理的规范化与常态化落地

制度层是“全域协同”治理体系落地的核心保障，高校需突破“重文本制定、轻执行落地”的建设误区，在现有制度框架基础上，完善权责清晰、流程闭环、动态适配的制度体系，推动“全域协同”治理从制度文本转化为常态化治理实践。

以《网络与信息安全管理办法》等核心制度为总纲，我们要聚焦 AI 教学应用、科研大数据共享、深伪内容防控等数智化新兴风险领域，逐一制定专项管理细则，填补制度空白。更重要的是，要把制度中原则性的要求，转化为可落地、可核查的标准化流程，明确系统上线、数据审批、安全处置等关键环节的操作规范和办理时限，让制度真正发挥作用，而不是停留在纸面上。

网络安全责任的落实，离不开全级次可追溯的考核与追责机制。我们要始终坚持“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，将网络安全工作纳入二级单位绩效考核和干部评优评先的核心指标，建立与职称评聘、年度考核直接挂钩的刚性约束。同时细化每个岗位的责任清单，健全分级分类追责制度，对责任落实不到位、整改不及时、引发安全事件的单位和个人严肃问责，构建起从责任传导、考核监督到追责问责的完整闭环。

针对信息化外包和第三方平台带来的安全隐患，需要建立覆盖准入、运维、退出全生命周期的管控体系。准入阶段，要把网络安全防护能力和数据合规资质作为硬性门槛，所有合作方必须签署安全保密协议和数据安全责任书。日常运维中，要严格管控第三方人员的系统权限，对所有操作行为进行审计，定期开展安全评估，核心数据的访问权限必须从严审批。合作终止时，要明确数据移交、权限注销的具体要求，并约定保密义务的延续期限，彻底消除外部治理链条上的风险盲区。

制度体系不是一成不变的，必须保持动态更新，才能持续适配治理需求。我们要密切跟踪《网络安全法》《数据安全法》等法律法规及行业监管要求的变化，定期对现有制度进行全面的合规性审查，及时修订完善相关内容，确保校内制度与上位法完全对标。同时，紧跟数智化技术的发展步伐，针对不断涌现的新型风险和应用场景，第一时间补充相应的制度规范，为“全域协同”的安全治理格局提供坚实的制度保障。

4.3. 平衡数据安全与利用，健全全生命周期的数据要素协同治理机制

数据是数智化时代的核心生产要素[10]，更是网络安全治理的重中之重。高校在推进数字化转型过程中，常常陷入“重保护轻利用”或“重流动轻安全”的两极化困境。我们要在“一数一源”制度实践的基础上，构建一套既能守住安全底线、又能释放数据价值的全生命周期协同治理机制，让数据安全与数智化发展相互促进、动态平衡。

“一数一源”是数据治理的根基。我们要依托核心业务系统打造权威数据源，搭建全校统一的数据中台和共享交换平台。通过这个平台，校内所有数据实现统一汇聚、标准化治理、合规共享和全流程溯源，从根本上解决长期存在的“数据烟囱”和“多头采集”问题。同时要建立健全数据质量管控机制，明确每个数据源主管部门的责任，确保数据准确、完整、及时，为后续的安全治理和价值挖掘打下坚实基础。

健全数据分类分级保护制度，实施差异化安全防护策略。数据分类分级能促进高校数据安全精细化管理和规范数据全生命周期管理[11]，依据国家数据安全相关标准，结合高校办学实际划分数据等级，针

对核心涉密数据、敏感个人信息、科研敏感数据、重要办学数据、公开公共数据，制定差异化的全流程管控规范。对师生敏感个人信息，严格遵循“最小化、匿名化”原则严控采集范围与访问权限；对科研敏感数据，实行全流程加密、访问审批与溯源审计，严防数据泄露风险。

第三，深化隐私计算技术应用，平衡数据共享与安全防护需求。隐私计算技术已成为解决大数据安全与隐私保护矛盾的重要方式[12]，针对高校教学科研、管理服务中的大数据共享需求，积极应用差分隐私、联邦学习等隐私计算技术，在不泄露原始数据的前提下实现数据合规共享与价值挖掘，破解“数据不敢共享、不能共享”的痛点，兼顾数据价值释放与师生个人信息权益保护。

4.4. 拓展多元主体联动，构建校内校外融合的全域协同治理生态

“全域协同”治理的核心，在于打破传统的主体壁垒。高校不能再局限于“校内闭环治理”的思维定式，要把治理边界从校内延伸到校外，打造校内全员参与、校外多元联动的治理格局，真正凝聚起各方力量。

师生是校园安全最直接的感受者，也是最有力的守护者。我们要把网络安全素养教育融入新生入学、教职工岗前培训和思政课程体系，常态化开展通识教育和专题讲座，筑牢师生的网络意识形态防线。同时要畅通安全隐患举报、漏洞上报的渠道，让师生从被动的“安全管控对象”，转变为主动的“治理核心主体”，形成人人有责、人人尽责的校内治理氛围。

校园安全治理离不开上级部门的指导和支持。我们要主动对接属地公安、网信、保密和教育主管部门，建立威胁情报共享、应急处置协同、案件联合查办的常态化工作机制。收到上级安全预警后，第一时间优化校内防护策略；发生重大安全事件时，第一时间上报并配合处置。积极参与监管部门组织的安全检查和培训演练，让校内治理标准与国家监管要求保持一致。

产教融合是提升治理能力的重要途径。我们要与国内领先的网络安全企业、科研机构建立长期战略合作，借助企业的技术优势和实战经验，升级校内安全防护体系，联合开展攻防演练、技术攻关和人才培养。同时发挥高校的学科和科研优势，共建网络安全实验室和实训基地，共同研发核心技术，实现技术支撑与人才培养的双向赋能。

构建区域性高校协同治理联盟。联合区域内兄弟高校建立网络安全协同治理联盟，实现威胁情报共享、防护经验交流、应急资源互助与技术能力共建。针对跨区域规模化网络攻击、钓鱼诈骗等共性风险开展联合防控与协同处置，破解单一高校技术能力、防护资源不足的痛点，形成区域联防联控合力，提升区域高等教育整体网络安全防护水平。

5. 结论

本文聚焦数智化时代高校网络安全传统碎片化治理的痛点，构建“技术－制度－价值”三层融合的“全域协同”治理理论框架，结合广州美术学院的制度化实践，梳理了组织、资产、数据、应用四大协同落地路径。研究表明，唯有实现技术、制度与价值的深度融合，才能破解传统治理困境。高校网络安全是教育强国建设的核心安全底座，需持续深化全域协同治理，为高等教育数智化转型筑牢安全屏障。

基金项目

中国高校产学研创新基金(2024MU039)；广州美术学院体制机制改革项目(20231125-030)。

参考文献

[1] 李国玮. 艺术类高校网络意识形态安全工作探究[J]. 大众文艺, 2024(11): 194-196.

[2] 朱晓飞. 基于网络安全新形势下的高校动态运营体系研究[J]. 网络安全技术与应用, 2025(10): 95-97.
[3] 顾坤坤, 郑伟发. 教育数字化转型背景下高校数据安全治理策略研究[J]. 网络安全技术与应用, 2025(11): 76-78.
[4] 林智钦. 高校机房网络安全管理分析[J]. 信息与电脑(理论版), 2024, 36(13): 176-178.
[5] 王淑荣, 崔昊. 数智时代高校网络意识形态的风险研判及对策[J]. 东北师大学报(哲学社会科学版), 2025(4): 19-26.
[6] 潘柱廷. 深化实施“人工智能 + 安全”, 筑牢智能安全新防线[J]. 中国信息安全, 2026(1): 49-50.
[7] 张长琳, 仝鑫, 佟晖, 杨莹. 面向网络安全领域的大语言模型技术综述[J]. 信息网络安全, 2024, 24(5): 778-793.
[8] 韩新敏, 贺瑞蕾. 电信网络诈骗犯罪治理研究[J]. 辽宁警察学院学报, 2026, 28(2): 28-35.
[9] 惠磊, 朱玉梅, 高艳玲. 信创背景下高校信息系统国产化改造关键技术研究[J]. 软件, 2025, 46(10): 129-131, 155.
[10] 陈小芳. 数智化信息技术赋能高校教育管理之研究[J]. 办公自动化, 2026, 31(4): 25-27.
[11] 张聪. 高校数据分类分级策略的探讨与实践[J]. 网络安全与数据治理, 2024, 43(6): 53-57.
[12] 李建华, 银鹰, 李思源, 林夕. 大数据安全与隐私计算技术综述[J]. 网络空间安全科学学报, 2024, 2(6): 1-15.