智媒时代青少年数字安全素养的体系化培育路径研究

熊 杨，李 杰

(重庆安全技术职业学院，巴南区 重庆 401320)

摘 要：随着人工智能、大数据、物联网等智能媒体技术的快速发展，青少年面临着前所未有的数字安全挑战。本研究基于智媒时代特征，构建了包含安全认知、技能实践、伦理责任三个维度的青少年数字安全素养框架，通过对川渝地区 10 所学校 500 名青少年的实证调研，发现当前青少年数字安全素养整体水平偏低，存在风险识别能力不足、防护技能缺失、责任意识淡薄等问题。研究提出了学校主导、家庭协同、社会参与的体系化培育路径，旨在为提升青少年数字安全素养、构建安全有序的数字环境提供理论指导和实践参考。

关键词：智媒时代；青少年；数字安全素养；体系化培育

基金项目：万州区社会科学重点课题《智媒时代青少年数字安全素养的体系化培育路径研究》（WZKT2025173），重庆安全技术职业学院校级教学改革项目《生成式人工智能融入信息技术课程体系的探索与实践》 (AQJG24-13)

DOI：doi.org/10.70693/rwsk.v2i5.437

一、智媒时代对青少年数字安全素养的影响分析

1.1 智媒时代的技术特征与安全挑战

智媒时代以人工智能、大数据、云计算、物联网等新兴技术为支撑，呈现出智能化程度高、数据融合度深、交互体验强、个性推荐精准等显著特征[1]，这些技术特征在为青少年带来便利的同时，也产生了新的安全风险：智能推荐算法基于用户行为数据进行内容推送，容易形成信息茧房效应，限制青少年的信息接触面，影响其认知的全面性和客观性，同时算法的“黑箱”特性使得推荐逻辑缺乏透明度，青少年难以理解和控制算法对其认知的影响[2]；生成式 AI 技术的发展使得深度伪造内容制作门槛大幅降低，虚假图片、视频、音频等内容在网络上大量传播，青少年面临辨别真伪信息的巨大挑战，容易被误导或欺骗[3]；智能设备和应用大量收集用户包括行为轨迹、兴趣偏好、社交关系等在内的敏感信息，而青少年缺乏充分的隐私保护意识和技能，个人信息面临泄露和滥用风险[4]；且智能媒体的高度个性化和沉浸式体验容易让青少年产生依赖性，过度使用可能导致注意力分散、社交能力下降、焦虑抑郁等心理健康问题[5]。

1.1 智媒时代青少年数字行为特征

通过对青少年数字行为的深入调研，发现智媒时代青少年呈现出多平台并行使用、内容创作参与度高、AI 工具使用频繁、风险感知能力弱等特征。青少年普遍同时使用多个社交媒体平台和应用程序，信息来源多样化但碎片化严重；超过 70%的青少年参与过内容创作和分享，但对版权和隐私保护意识不足；近 60%的青少年使用过豆包、文心一言等 AI 工具，但对 AI 生成内容的可靠性缺乏批判性思考；仅有 32%的青少年能正确识别网络诈骗信息，28%能识别深度伪造内容。

二、青少年数字安全素养核心要素框架构建

2.1 理论基础与研究方法

作者简介：熊 杨(1999—)，女，硕士研究生，研究方向：职业教育和数字媒体。

李 杰(1998—)，男，工学硕士，研究方向：职业教育、计算机视觉。

本研究基于媒介素养理论、数字公民理论和风险社会理论，采用文献分析法、德尔菲法和因子分析法，构建青少年数字安全素养核心要素框架。通过对国内外相关研究的梳理，邀请 10 位专家进行两轮德尔菲调查，最终确定框架结构。

2.2 数字安全素养核心要素

构建青少年数字安全素养三维九要素框架模型，如图 1 所示。

图 1 青少年数字安全素养三维框架模型

安全认知维度要求具备风险识别能力、安全知识储备与威胁评估能力，具体而言即能够识别网络诈骗、恶意软件、虚假信息、深度伪造等各类数字安全威胁，掌握基本的网络安全知识、法律法规和防护原理，同时能评估不同数字环境和行为的安全风险等级；技能实践维度包含防护操作技能、应急响应能力与安全创作能力，需掌握具体的安全防护操作方法和技术手段，具备面对安全事件时的处置和求助能力，并且在创作和分享数字内容时遵循安全规范；伦理责任维度则强调法律法规意识、社会责任感与伦理道德观念，要了解并遵守数字环境相关的法律法规，承担维护网络空间安全的社会责任，在数字环境中坚持正确的价值观和道德标准。三个维度相互关联、相互促进，共同构成青少年在智媒时代应具备的核心安全素养。

三、青少年数字安全素养现状调研与分析

3.1 调研设计与实施

3.1.1 调研方法与样本

本研究采用随机抽样方法，调研对象为 13-22 岁的青少年，包括初中生、高中生和大学生三个群体，发放问卷 500 份，回收有效问卷 477 份，有效率 95.4%。同时，采用深度访谈方法，对 10 名学生、10 名家长、10 名教师进行个别访谈，深入了解数字安全素养培育的现状和需求。

3.1.2 调研工具与指标

基于构建的三维九要素框架，开发《青少年数字安全素养评估量表》，包含 45 个题项，采用李克特 5 点计分法。量表经过信效度检验，Cronbach's α 系数为 0.892，具有良好的信度和效度。

3.2 调研结果分析

调研结果显示，青少年数字安全素养整体水平处于中等偏下水平，平均得分 3.18 分（满分 5 分）。具体表现如表 1 所示。

表 1 青少年数字安全素养各维度得分情况

维度	要素	平均分	标准差	水平等级
安全认知维度	风险识别能力	3.12	0.86	中等偏下
	安全知识储备	3.25	0.79	中等
	威胁评估能力	3.08	0.92	中等偏下
	维度平均	3.15	0.72	中等偏下
技能实践维度	防护操作技能	2.95	0.94	中等偏下
	应急响应能力	3.18	0.88	中等
	安全创作能力	3.22	0.81	中等
	维度平均	3.12	0.78	中等偏下
伦理责任维度	法律法规意识	3.35	0.76	中等
	社会责任感	3.28	0.83	中等
	伦理道德观念	3.41	0.74	中等
	维度平均	3.35	0.69	中等
总体平均		3.18	0.71	中等偏下

3.3 主要问题与挑战

3.3.1 风险识别能力不足

调研发现，仅有 34.2%的青少年能够正确识别钓鱼网站，29.8%能够辨别深度伪造内容。面对复杂的网络环境，青少年缺乏有效的风险识别方法和经验。案例分析：在模拟测试中，向受访者展示了一个制作精良的虚假购物网站，80%的青少年表示会在该网站输入个人信息和银行卡信息进行购买。

3.3.2 防护技能掌握不足

超过 60%的青少年从未更改过设备的默认安全设置，42%的青少年使用弱密码或重复密码，仅有 18%的青少年启用了双因素认证功能。

3.3.3 批判性思维缺乏

青少年对 AI 生成内容普遍缺乏批判性思维，67%的青少年表示“很难区分 AI 生成的内容和人类创作的内容”，仅有 25%的青少年会主动验证网络信息的准确性。

3.3.4 法律法规认知模糊

调研显示，仅有 41%的青少年了解《网络安全法》的基本内容，35%了解《数据安全法》，对网络行为的法律边界认识不清。

3.3.5 教育支持体系不完善

学校层面：仅有 17.3%的学校开设了专门的网络安全或数字素养课程，大部分学校将相关内容零散地融入信息技术课程中。家庭层面：能够为孩子提供数字安全指导的家长仅占 26.8%，家长自身数字安全素养水平普遍不高。社会层面：优质的青少年数字安全教育资源相对匮乏，专业的教育服务机构较少。

四、青少年数字安全素养体系化培育路径研究

4.1 培育路径的理论基础

基于生态系统理论、协同教育理论和终身学习理论，构建青少年数字安全素养体系化培育路径[6]。生态系统理论强调个体发展受到多层次环境因素的影响；协同教育理论重视多元主体的协同作用；终身学习理论突出持续学习的重要性。

4.2 学校主导的教育路径

4.2.1 课程体系构建

根据青少年认知发展特点，设计分阶段递进式课程体系。并将数字安全教育融入语文、数学、科学、社会等学科教学中。

表 2 青少年数字安全素养课程体系设计

学段	课程模块	主要内容	课时安排
初中阶段	数字安全基础	网络安全常识、密码管理、隐私保护	18 课时/学期
	风险识别入门	网络诈骗识别、恶意软件防范	12 课时/学期
	文明上网行为	网络礼仪、数字伦理基础	6 课时/学期
高中阶段	智能时代安全	AI 风险识别、算法理解、深度伪造防范	20 课时/学期
	数据隐私保护	个人信息保护、数据权利认知	16 课时/学期
	法律法规素养	网络安全法律、数字权利义务	10 课时/学期
大学阶段	智能技术安全前沿	人工智能安全、大数据隐私计算、区块链应用安全、物联网风险防控	36 课时/学期
	高级法律与数字实务	网络安全法深度解读、数字取证、跨境数据流动规制、知识产权与数字创新	32 课时/学期
	伦理领导力与治理	数字伦理决策、组织数据治理、安全架构设计、网络危机公关与沟通	30 课时/学期

4.2.2 教学模式创新

教学模式创新可从多维度推进，其中情境体验式教学通过构建真实的网络安全情境助力学生在体验中学习，如建设网络安全体验中心以模拟各种安全威胁场景，开发网络安全游戏实现寓教于乐，同时组织黑客马拉松活动培养学生的安全防护技能；案例分析教学法聚焦典型网络安全案例开展深入分析，具体包括剖析近期发生的网络安全事件、讨论青少年身边的真实案例，还会邀请网络安全专家分享实战经验；项目制学习模式则组织学生参与实际的安全项目，例如开展校园网络安全检查项目、策划数字安全宣传活动，以及进行安全防护工具开发体验。

4.2.3 师资队伍建设

主要围绕专业能力提升与资格认证制度两大方向展开，其中专业能力提升需建立教师数字安全素养培训体系，具体包括定期组织网络安全技术培训、开展数字素养教育教学方法研修，同时搭建教师学习交流平台以促进经验共享；资格认证制度方面，需建立数字安全教育教师资格认证制度，不仅要制定明确的教师能力标准和认证流程，还要建立持续教育和能力更新机制，并且完善相应的激励保障措施，为师资队伍建设提供制度支撑。

4.3 家庭协同的培育路径

4.3.1 家长教育与培训

一方面需推进家长数字安全素养提升计划，针对家长群体开展专门培训，具体包括开设家长数字安全讲堂、制作家庭数字安全指导手册以及建立家长学习交流群组，另一方面要建立家校协同的教育机制，通过定期举办家校数字安全教育沙龙、开展亲子数字安全实践活动、搭建家校信息沟通平台实现家校联动；

4.3.2 家庭环境优化

一是指导家庭制定合理的数字家庭规则，明确上网时间和内容限制，建立设备使用的安全规范，同时营造开放沟通的家庭氛围，二是推荐适合的家庭数字安全工具，涵盖家长控制软件的合理使用、网络过滤和监控工具的配置，以及安全浏览器和防护软件的推荐。

4.4 社会参与的支持路径

4.4.1 政府统筹协调

需从政策与资源两大关键层面发力：一方面聚焦政策制定与实施，具体包括制定青少年数字安全教育发展规划，出台相关法规和标准规范以明确方向与准则，建立跨部门协调工作机制保障工作高效推进，同时加强执法监管力度筑牢安全底线；另一方面强化资源投入保障，通过设立专项教育发展基金提供资金支持，加强基础设施建设投入完善硬件条件，支持优质教育资源开发丰富教学内容，还需完善师资培养保障体系，为教育工作开展提供人才支撑。

4.4.2 企业社会责任

一是聚焦技术支持与服务，主动承担社会责任，具体包括开发青少年友好的安全产品、提供专业的技术支持与服务、参与青少年数字安全教育内容及相关平台的开发，同时积极支持公益性质的青少年数字安全教育活动开展；二是注重行业自律与规范，通过制定专门的青少年保护行业标准明确行为准则，建立内容审查和过滤机制防范不良信息传播，完善用户举报和问题处理流程及时响应安全需求，并且进一步加强数据保护和隐私安全管理，为青少年营造安全的数字环境。

4.4.3 社会组织参与

一方面依托专业机构提供多元支持，其中网络安全研究机构负责提供技术指导，教育研究机构开展相关理论研究，培训机构提供专业服务，评估机构则开展效果评价，形成专业领域的协同支撑；另一方面鼓励公益组织积极行动，通过开展数字安全宣传教育活动普及安全知识，组织志愿服务和公益项目拓展实践场景，建立青少年保护网络织密安全防护网，推动社会各界对青少年数字安全问题的关注与参与，凝聚多方合力。

五、结论

本研究通过分析智媒时代技术特征与安全挑战，构建青少年数字安全素养理论框架、调研现状并设计体系化培育路径，主要结论如下：一是智媒时代算法推荐、深度伪造等新技术带来复杂安全风险，对青少年数字安全素养要求更高，需其具备更强风险识别能力、批判性思维与防护技能；二是当前青少年数字安全素养整体待提升，在风险识别、防护技能、法律意识上存在不足，安全教育支撑体系尚不完善；三是体系化培育路径有效，构建学校主导、家庭协同、社会参与的协同育人机制可形成教育合力，提升培育效果。

参考文献：

[1] 潘虹莉.智媒生态系统构建——基于大数据与人工智能的媒体融合新路径[J].新闻文化建设,2025,(07):54-56.DOI:10.20253/j.cnki.cn10-1677/g.2025.07.042.

[2] 虞鑫,王金鹏.重新认识“信息茧房”——智媒时代工具理性与价值理性的共生机制研究[J].新闻与写作,2022,(03):65-78.

[3] 何宇华,李霞.生成式人工智能虚假信息治理的新挑战及应对策略——基于敏捷治理的视角[J].治理研究,2024,40(04):142-156+160.DOI:10.15944/j.cnki.33-1010/d.20240618.001.

[4] 刘楠楠.未成年人模式的现实困境、改革方向与实践进路——以未成年人的数字安全与数字素养发展为要[J].青少年法治教育,2025,(03):24-30.

[5] Mustafa S ,Hatice D Y ,Gül Ö , et al.The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender[J].Online Information Review,2024,48(5):983-1001.DOI:10.1108/OIR-03-2023-0122.

[6] 吴军其,刘萌.家校社协同学生数字素养教育：价值意蕴、联动逻辑与实践进路[J].当代教育论坛,2025,(02):34-43.DOI:10.13694/j.cnki.ddjylt.20240929.002.

Research on the Systematic Cultivation Path of Teenagers' Digital Security Literacy in the Era of Smart Media

Xiong Yang, Li Jie

Chongqing Vocational Institute of Safety Technology,ChonngQing,China

Abstract: With the rapid development of intelligent media technologies such as artificial intelligence, big data and the Internet of Things, teenagers are facing unprecedented digital security challenges.Based on the characteristics of the intelligent media era, this study constructed a framework of digital security literacy for teenagers, which includes three dimensions: security cognition, skill practice, and ethical responsibility. Through empirical research on 500 teenagers from 10 schools in Sichuan and Chongqing regions, it was found that the overall level of digital security literacy among teenagers is relatively low at present, with problems such as insufficient risk identification ability, lack of protection skills, and weak sense of responsibility.The research proposed a systematic cultivation approach led by the school, coordinated by the family, and involving the participation of society, aiming to provide theoretical guidance and practical references for enhancing the digital security literacy of teenagers and building a safe and orderly digital environment.

Keywords: intelligent media era;adolescents;digital safety literacy;systematic cultivation