Advances in Social Sciences 社会科学前沿, 2026, 15(1), 673-684
Published Online January 2026 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2026.151082

Hans汉斯

新时代加强大学生网络安全观培育的价值意蕴

闵心怡

南昌航空大学马克思主义学院，江西 南昌

收稿日期：2025年12月5日；录用日期：2026年1月15日；发布日期：2026年1月27日

摘　要

在新时代背景下，加强大学生网络安全观培育具有重要且多维的价值。在宏观层面，大学生网络安全观培育呼应了国家发展与安全战略，是维护总体国家安全、建设网络强国、应对国际网络空间竞争的必然要求。在中观层面，大学生网络安全观培育体现了高等教育现代化的使命，通过落实立德树人、优化校园网络治理和创新安全教育，为人才培养提供坚实支撑。在微观层面，大学生网络安全观培育契合学生成长的内在需求，不仅为其全面发展保驾护航，更有助于提升其网络风险防范能力与数字时代公民责任感。

关键词

网络安全，网络安全观培育，价值意蕴

The Value Implications of Strengthening Cybersecurity Awareness among University Students in the New Era

Xinyi Min

School of Marxism, Nanchang Hangkong University, Nanchang Jiangxi

Received: December 5, 2025; accepted: January 15, 2026; published: January 27, 2026

Abstract

Against the backdrop of the new era, strengthening cybersecurity awareness among university students holds significant and multidimensional value. At the macro level, cultivating such awareness aligns with national development and security strategies, serving as an imperative requirement for safeguarding overall national security, building a cyber powerhouse, and addressing international competition in cyberspace. At the meso-level, it fulfils the mission of modernising higher

文章引用: 闵心怡. 新时代加强大学生网络安全观培育的价值意蕴[J]. 社会科学前沿, 2026, 15(1): 673-684.
DOI: 10.12677/ass.2026.151082

education by implementing moral education, optimising campus cyber governance, and innovating security education, thereby providing robust support for talent cultivation. At the micro-level, it aligns with students' intrinsic developmental needs, safeguarding their holistic growth while enhancing their capacity to mitigate cyber risks and fostering civic responsibility in the digital age.

Keywords

Cybersecurity, Cultivation of Cybersecurity Awareness, Value Implications

1. 引言

数字时代下，网络空间既是民众的精神家园，更是国家主权的数字延伸。网络安全已非单纯技术问题，而是关乎国家主权、安全与发展利益的战略议题，习近平总书记深刻提出“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”[1]，揭示了网络安全在总体国家安全中基础性支撑地位与全局性战略价值。

本文所探讨的“网络安全观”，并非孤立的概念，而与数字素养、媒介与信息素养及网络心理等领域紧密相连。联合国教科文组织将“在线保护个人数据、隐私及识别风险”明确列为公民核心数字素养[2]；而媒介与信息素养的培养旨在提升公众对媒介信息的辨别与筛选能力，从而抵御低俗信息与消费主义对个体认知的侵蚀[3]；国内网络心理学研究指出，大学生的网络心理如在线去抑制效应、社会临场感与从众心理等对其网络行为影响程度深，从而对其身心健康造成强烈影响[4]。本文将“网络安全观”置于此框架下，将其界定为一种综合性的数字公民素养，它不仅指对网络威胁的警惕意识，更涵盖知识、技能、态度、价值观、伦理意识以及最终指向的行为习惯。大学生作为国家未来中坚力量，既是数字时代主要参与者，也因安全意识待提升易受网络风险侵蚀，其网络安全观更与国家网络安全防线构建紧密相关。

然而，现实调查(本文调查数据样本 N = 1040，KMO 值为 0.901，KMO 取样适切性量数为 0.957，Bartlett 球形度检验的卡方值为 5822.199，Sig.值为 0.000，表明样本数据适合做探索性因子分析。具有比较理想的信度和效度。)显示，当前部分大学生对网络安全基础概念认知模糊，对法律法规的理解多停留在表面；在行为上存在网络信息轻信度高、网络安全行为风险较大等现象；一项国际调查研究同样显示，尽管新时代大学生是“数字原住民”，但其网络安全知识匮乏、风险行为普遍，认知与行为之间存在显著鸿沟[5]。而在国际上，将网络安全观培育提升至国家战略与国民素养核心构成的高度，已成为全球主要经济体的普遍共识与共同实践。从欧盟的“加强网络安全”项目、美国的“国家网络安全教育计划”(NICE)，到新加坡将网络素养深度融入国民教育课程与评估体系，国际经验清晰地表明：系统化、前置化的网络安全观培育，是应对复杂数字风险、塑造负责任数字公民、赢得未来数字竞争的基础性工程。因此，在新时代总体国家安全观指引下，探讨大学生网络安全观培育的价值意蕴，明确其在国家战略、高等教育、个体成长中的作用，既是应对网络安全形势的现实需要，也是培养民族复兴大任新人的必然要求。

2. 宏观维度：国家发展与安全战略的时代诉求

大学生网络安全观培育是一项承载国家战略意志、关乎发展全局的系统性工程。其核心价值在于，

它通过对未来社会中坚力量——大学生群体的素养塑造，前瞻性地筑牢国家数字生存与发展的安全根基，并战略性塑造国家在网络时代的核心竞争力。这绝非孤立的校园教育活动，而是国家总体安全观在网络空间的具体实践、网络强国战略在人才储备与公民素养维度的关键落点，以及国家参与并引领全球数字治理进程的基础性投入。

2.1. 维护国家总体安全的重要屏障

2.1.1. 落实总体国家安全观的基础性工程

从国家安全战略的角度来看，大学生网络安全观培育是筑牢数字时代国家安全屏障的关键举措。大学生作为网络原住民，其安全意识和防护能力直接影响国家网络安全整体水平。通过系统化的网络安全教育，能够使大学生在复杂的网络环境中保持政治敏锐性，自觉抵制西方意识形态渗透，维护国家网络空间主权，为维护国家网络主权和安全构筑坚实的青年防线。从社会协同维度看，大学生网络安全观培育是构建全民网络安全防线的重要支点。大学生群体具有较强的影响力和示范效应，通过提升这一群体的网络安全素养，可以辐射带动全社会网络安全意识的整体提升，形成维护网络安全的强大社会合力。这种以点带面的教育效果，能够有效夯实国家网络安全的社会基础，为总体国家安全观的落实提供广泛的社会支持。

2.1.2. 防范网络意识形态渗透的关键防线

当前网络意识形态领域面临着前所未有的复杂挑战。随着数字技术的快速发展，西方意识形态渗透呈现出新的特征。在传播方式上，这种渗透通过算法推荐和社交媒体的“信息茧房”效应，使特定价值观的传播更具针对性和隐蔽性；在内容呈现上，它将意识形态内容嵌入影视作品、网络游戏等文化产品中，以娱乐化形式进行软性渗透；在议题设置上，它借助国际热点事件构建话语陷阱，制造认知偏差。这些新型渗透手段对大学生群体的价值观形成产生了深远影响。特别是在全球化背景下，网络意识形态已从显性的政治宣传转向隐性的文化渗透。有学者指出“互联网是当代最锐利的信息传媒载体，意识形态是其本质属性之一”[6]，在此等状况下，对大学生培育正确的网络价值观念尤为重要。

培育大学生网络安全观是抵御错误思潮渗透的主动防御机制，健全的网络安全观是维护主流意识形态安全的重要保障。培育网络安全观的核心在于使大学生掌握三大关键能力：一是信息甄别能力，能够识别虚假新闻和隐蔽的价值诱导；二是批判思维能力，能够解构信息背后的意识形态框架；三是价值判断能力，基于国情和历史形成独立的价值立场。通过强化对大学生的网络安全观教育，在认知维度可以帮助其树立网络安全形势的清醒认识，在价值维度上促成其社会主义核心价值观的内化，在实践维度培养其负责任的网络行为规范。这种以主体素养提升为基础的防御机制，能够从源头上增强抵御非主流意识形态渗透的免疫力。通过系统化的网络安全教育，能够提升大学生的政治鉴别力和价值判断力，有利于其在网络空间主动识别和抵制错误思潮，筑牢思想防线；有利于增强其对主流价值观的认同，确保社会主义核心价值观在网络空间的主导地位。

2.1.3. 保障关键信息基础设施安全的战略支撑

大学生网络安全观培育通过构建多层次的安全人才体系，为关键信息基础设施安全提供战略性支撑。根据《关键信息基础设施安全保护条例》第 2 条的规定，关键信息基础设施是指公共通信和信息服务、能源、交通水利、金融、公共服务、电子政务、国防科技工业等 8 大重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。关键信息基础设施安全是国家安全的重要保障，一方面，关键信息基础设备所涉及的各个领域是世界各国的竞争博弈的核心焦点；另一方面，互联网技术本身存在脆弱性，而大数据、人工智能等

新兴技术的运用，使得关键信息基础设施面临的威胁持续增加。互联网时代以来，世界出现的关键信息基础设施安全恶性事件时有发生。在严峻的安全风险和隐患面前，重点保护关键信息基础设施的必要性不言而喻。2024 年网络安全产业人才发展报告显示，我国网络安全领域正面临人才与技能双重缺口扩大的挑战，主要表现为人才缺口持续扩大、技能缺口逐渐明显和 AI 人才需求激增。通过系统化的网络安全教育，可以培养三类急需人才：一是具备基础安全意识的普通运维人员，能够识别常见网络威胁；二是掌握专业技能的工程师，可进行系统安全防护；三是具有战略视野的管理者，能够统筹安全体系建设，能有效缓解我国网络安全领域的人才缺失。从长效机制维度看，大学生群体的网络安全素养提升会产生显著的正外部性效应，对培养专业人才、维护国家安全和经济社会发展具有深远意义。

2.2. 推进网络强国建设的必然要求

2.2.1. 实现“十四五”数字中国战略的人才保障

古往今来的历史经验表明，“得人者兴，失人者崩”。人才始终是富国之本、兴邦大计，是推动社会发展的“第一资源”。网信领域作为技术密集型和创新密集型领域，其竞争归根结底是人才竞争。

一方面，大学生网络安全观培育有利于强化国家安全意识，筑牢网络空间防线。网络安全是国家安全的重要组成部分，大学生作为网络空间的重要参与者和未来建设者，其网络安全观的培养直接关系到国家网络空间的安全稳定。通过系统化的网络安全教育，引导大学生树立正确的网络安全意识，增强对网络威胁的识别与防范能力，使其在未来的职业发展中能够自觉维护国家网络主权和数据安全，成为网络强国建设的坚实力量。另一方面，培育大学生网络素养有利于促进创新人才培养，服务网络强国战略。网信领域的竞争本质上是人才的竞争，而网络安全人才是其中的关键力量。通过加强大学生网络安全教育，可以发掘和培养一批具备扎实技术能力、创新思维和战略眼光的网络安全专业人才，为突破关键核心技术、构建自主可控的网络安全体系提供智力支持。同时，良好的网络安全观能够激发大学生的创新潜能，推动其在人工智能、大数据、区块链等新兴领域的研究与应用，为数字中国建设贡献智慧和力量。

2.2.2. 提升国家网络空间国际话语权的根基

网络空间国际话语权是国家软实力的重要体现，有学者指出“在百年变局与世纪疫情叠加的大变革时期，网络空间话语权的争夺已然成为大国博弈的重要方面”，而网络安全观的培育是构建这一话语权的重要根基。大学生作为未来国家建设的中坚力量，其网络安全意识的强弱、网络素养的高低，直接影响国家在全球网络安全合作中的话语能力。一方面，大学生网络安全观培育有利于强化国家网络空间安全的“技术自主性”。国际话语权的根基在于技术实力。当前，尽管我国在网信事业取得诸多成就，但全球网络空间的核心技术、关键基础设施和标准体系仍由少数发达国家主导。系统培育大学生的网络安全观，能够激发其投身网络安全核心技术研发的使命感，推动自主可控技术的突破，减少对外依赖。只有具备强大的技术自主能力，国家才能在国际网络空间博弈中掌握主动权，避免在规则制定和技术标准竞争中被边缘化。另一方面，大学生网络安全观培育有利于增强国家网络空间战略的“道义影响力”。国际话语权不仅依赖硬实力，也取决于价值观的吸引力。通过培养大学生的网络安全观，使其具备正确的网络主权意识、数据安全伦理和全球协作精神，能够向国际社会传递负责任、开放合作的网络治理理念。在国际网络合作事务中，具备网络安全素养的专业人才可以更好地阐释中国方案，增强我国在网络空间治理中的道义感召力。

2.2.3. 推动数字技术创新发展的素质储备

在建设网络强国的时代背景下，大学生网络安全观培育是推动数字技术创新发展的必然选择有学者指出通过长期、持续开展青少年数字素养培育，有助于使其得以在数字环境中从容发展全方面的能力[7]。

首先，大学生网络安全观培育有助于大学生形成安全与创新并重的发展理念。在数字经济时代，安全不再是创新的约束条件，而是技术发展的内在要求。通过网络安全教育，能够帮助学生树立“没有网络安全就没有创新发展”的基本认知，使其在技术研发过程中自觉将安全要素融入创新实践。这种理念的形塑，既避免了为追求创新速度而忽视安全风险的冒进倾向，也防止了因过度保守而阻碍技术突破的消极思维，为数字技术创新提供了健康可持续的发展导向。其次，大学生网络安全观培育能够强化技术创新的伦理意识。技术创新不能脱离伦理约束而独立存在，网络安全教育通过培养风险意识、责任意识，为学生划定技术创新的伦理边界。真正的技术创新不仅要考虑技术可行性，还要评估社会影响；不仅要追求功能突破，还要确保安全可控。这种伦理意识的培育，使学生在技术研发过程中能够自觉把握创新与规范的辩证关系，既保持开拓进取的创新精神，又坚守安全底线的责任担当。最后，网络安全观培育可以强化创新人才的责任担当。数字技术的发展关乎国家安全和社会稳定，网络安全教育通过增强学生的国家安全意识和社会责任感，培养其“技术报国”的使命担当。这种责任意识促使学生在技术创新中自觉维护国家网络主权和数据安全，主动将个人发展融入国家战略需求，在网络强国建设中贡献智慧力量。

3. 中观维度：高等教育现代化的使命担当

3.1. 落实立德树人根本任务的核心环节

立德树人是高等教育的根本任务，数字时代的“立德”不仅包含传统道德素养的培育，更需强化大学生在网络空间的价值判断、责任意识与政治自觉；“树人”则要求培养能主动应对网络风险、守护网络文明的时代新人。大学生网络安全观培育以“安全认知 + 价值引领”为双主线，将“德”的培育与“能”的提升融入网络场景，成为新时代落实立德树人根本任务的核心环节。

3.1.1. 培养社会主义建设者政治敏锐性的必然要求

当前网络空间已成为意识形态斗争的重要场域，有学者指出，在网络空间不同的利益主体有不同的利益诉求，除主流媒体外，一些动机不纯的媒体“通过歪曲历史、丑化党的形象等卑劣伎俩在网络空间大肆宣扬、传播所谓的‘普适价值’，宣传错误的思想观念和政治观点、不良的价值理念和社会思潮”[8]，试图冲击大学生的政治认知。作为未来社会主义建设的中坚力量，大学生的政治敏锐性直接关系到国家意识形态安全与政治稳定。大学生网络安全观培育并非单纯的“技术安全教学”，而是将政治素养培育融入风险认知：通过解析“网络意识形态渗透的典型案例”、讲解“网络空间主权与国家政治安全的关联”，引导大学生辨别网络信息中的政治陷阱，认清“技术中立”表象下的意识形态操控，进而提升对“有害信息”的政治判断力、政治领悟力与政治执行力。这种培育模式从“被动防御”转向“主动辨识”，是确保大学生成长为“政治清醒、立场坚定”的社会主义建设者的必然要求，也是立德树人在“政治维度”的重要体现。

3.1.2. 强化社会主义核心价值观网络传播的主渠道

社会主义核心价值观的传播需适配数字时代的载体与语境，而高校作为价值观培育的主阵地，其网络传播效能直接影响立德树人的成效。大学生网络安全观培育为核心价值观传播提供了“场景化、实践化”的载体。一方面，培育过程中可结合宣传“网络诚信”如抵制虚假信息、不参与网络欺诈阐释“诚信”价值观，结合讲解“网络法治”如遵守《网络安全法》、不实施跨境网络攻击阐释“法治”价值观，将抽象的核心价值观转化为大学生可感知、可践行的网络行为准则，避免价值观传播的空洞化；另一方面，大学生作为网络内容的生产者与传播者，其经培育形成的安全观与价值观会同步融入网络实践，可带动校园乃至社会层面的核心价值观传播，形成“高校引领－学生实践－社会辐射”的传播链条。这种

以安全观培育纽带的传播模式，强化了高校作为核心价值观网络传播“主渠道”的功能，让立德树人在价值维度落地生根。

3.1.3. 构建“大思政”育人格局的创新切入点

“大思政”育人格局强调“全员育人、全程育人、全方位育人”，需打破学科壁垒、整合育人资源，实现“思政课程”与“课程思政”的协同。大学生网络安全观培育天然具备跨学科、强联动的属性，可成为破解“思政教育碎片化”问题的创新切入点。从“课程协同”看，其内容可融入思政课、专业课程通识课程，实现“思政 + 专业”的深度融合；从“资源整合”看，高校可联动网信部门、网络安全企业、公安机构等校外资源，通过专家讲座、实践实训、案例研讨等形式，将社会大课堂引入校园，形成“校内教师 + 校外专家”的全员育人队伍；从过程覆盖看，培育可贯穿大学生“入学－在校－毕业”全周期，实现“全程育人”。这种培育模式以“网络安全”为纽带，打通了“课程、资源、过程”的育人壁垒，为“大思政”格局的构建提供了可操作、可复制的实践路径，是立德树人在“机制维度”的重要创新。

3.2. 优化高校网络治理生态的关键举措

高校网络治理生态是高等教育现代化治理体系的重要组成部分，其核心在于实现校园网络秩序稳定、师生网络权益保障、网络育人功能凸显的协同统一。舆情、诈骗、信息泄露等一旦在校园出现，将会给高治治理环境带来极大破坏。而大学生网络安全观培育可成为破解这些难题、优化高校网络治理生态的关键之举。

3.2.1. 净化校园网络舆情环境的治理抓手

习近平总书记曾经多次强调做好网络意识形态工作的重要性，他指出“做好网上舆论工作是一项长期任务，要创新改进网上宣传，运用网络传播规律，弘扬主旋律，激发正能量”[9]。校园网络舆情具有内容领域多样且复杂、传播形式多元且速度快、社会关注度高且信息复杂、舆情主客体统一性且不成熟等特点[10]，一旦出现虚假信息、极端言论如校园管理谣言、学术不端不实指控，易引发学生群体焦虑、对立，甚至冲击校园正常教学秩序。传统高校网络舆情治理多依赖事后管控如删除违规内容、封禁账号，难以从根源上遏制负面舆情滋生，而大学生网络安全观培育为舆情治理提供了事前预防、事中引导的主动抓手。

大学生网络安全观培育通过引导学生掌握信息溯源方法与舆情辨别逻辑，本质是为校园舆情治理提供根源性认知赋能。传统校园舆情治理的短板在于，学生因缺乏系统的信息辨别能力，易成为负面舆情的被动传播载体，导致治理陷入“事后管控－反复出现”的循环。而培育过程中对信息真伪判断能力、舆情操控手段识别能力的塑造，能帮助学生突破盲目跟风的认知局限，建立理性审视信息的思维惯性——这种认知升级不仅让学生自身远离无意识传谣，更从源头减少负面舆情的传播节点，实现舆情治理从被动应对风险向主动阻断风险的转变，为校园舆情生态筑牢“认知防线”，契合高校治理中预防优于管控的核心价值取向。这种以培育为基础的治理模式，将大学生从舆情被动接受者转化为舆情主动治理者，既降低了高校舆情管控的行政成本，又通过朋辈引导增强了舆情治理的公信力，成为净化校园网络舆情环境的长效抓手。同时，培育过程中对学生理性发声意识的强化与舆情参与引导，核心是激活校园舆情治理的多元主体价值。高校舆情治理的现代化目标，在于打破单一官方主导的传统模式，构建官方－学生协同共治的格局。通过培育大学生网络安全观，有利于推动学生主动抵制极端化言论、参与舆情引导，实质是将学生从舆情受众转化为治理参与者。一方面，学生的主动参与能填补官方治理的空缺，降低单纯依赖行政管控的成本，提升治理效率；另一方面，基于朋辈身份的舆情引导更易获得学生群体的信任，

避免官方管控可能引发的抵触情绪，增强舆情治理的公信力与接受度，从而有效遏制负面舆情的扩散升级，维护校园秩序稳定——这种“官方引导 + 学生自治”的协同模式，正是高校网络治理生态向多元协同、高效有序升级的关键价值体现，也呼应了高等教育现代化中激发主体能动性的治理理念。

3.2.2. 预防校园网络诈骗与信息泄露的治本之策

当前高校网络治理面临校园网络诈骗与个人信息泄露问题日益严峻，其中，校园贷、虚假兼职等诈骗手段层出不穷，而学号、身份证等敏感信息的非法交易也时有发生。这些安全问题不仅造成大学生直接的经济损失，更可能引发信用危机、身份盗用等严重后果。究其根源，大学生安全意识薄弱与防护能力不足是问题关键。传统的安全宣传教育往往停留在零散的警示海报或偶尔的讲座上，难以形成持久效果。相比之下，系统化的网络安全观培育能够从认知到行为实现全方位提升。

大学生网络安全观培育对大学生开展针对校园诈骗与信息泄露的高频场景开展专项教学，其价值并非单纯讲解风险案例，而是通过解析校园贷的低息陷阱与暴力催收危害、拆解兼职刷单先甜后苦的诈骗逻辑，帮助大学生穿透“利益诱惑”的表象，看清风险本质，进而建立风险预判意识——这种意识的建立，能让大学生在面对类似诱惑时，主动启动“风险筛查”思维，避免因认知盲区陷入被动受害困境。同时，培育中的实操训练教学如个人信息分级保护方法、可疑链接检测技巧、诈骗证据留存流程等，其价值在于将抽象的安全认知转化为具体的防护能力，推动大学生从不知道如何防范转向掌握主动防范技能，为后续的安全行为提供认知支撑，从根源上降低个体遭遇诈骗与信息泄露的概率。这不仅能让大学生在日常网络行为中主动规避风险，减少个人安全漏洞，更能降低高校的治理成本——相较于反复开展碎片化宣传、事后处理诈骗纠纷，培育带来的“主动防护习惯”具有更强的持续性，能从行为层面减少风险发生的可能，提升校园网络治理效率。

3.3. 推动安全教育体系创新的实践突破

传统高校安全教育体系面临“传统模式滞后、供给与需求脱节、育人协同不足”等问题，难以适配数字时代大学生的安全需求。当前高校网络安全教育面临供给侧与需求侧的显著错配，近 70%的大学生明确表示更倾向于“实践导向型”或“理论结合实践”的教育方式，这反映了数字原住民对可操作、场景化知识的强烈需求。然而，学生对现有教育的评价却指向了另一面：高达 45.77%的学生认为教育“缺乏实践环节，如模拟演练”，40.77%的学生认为“教学内容过于理论化，缺乏实际案例”，同时超过三分之一的学生指出教育“形式单一”和“内容陈旧”。这种供需矛盾导致教育参与度与实效性不佳，大学生网络安全观培育以“系统性、精准化、融合性”为核心特征，在推动安全教育体系创新中展现出关键实践价值，成为突破传统教育局限、完善育人体系的重要支撑。

3.3.1. 破解传统安全教育碎片化困境的改革方向

传统高校安全教育多以碎片化宣传为主，如学期初的安全讲座、节假日的海报提醒、突发事件后的临时通知等，内容上缺乏逻辑关联，形式上依赖单向灌输，导致学生对安全知识的认知零散化、表面化，难以形成系统的安全思维与持续的防护意识。大学生网络安全观培育通过系统化教育，正在打破这种碎片化困境。一方面，培育构建模块化、递进式的内容体系，将网络安全知识拆解，从基础概念到实操应用逐步深入，形成完整的知识链条，让学生不仅“知其然”，更“知其所以然”；另一方面，培育采用常态化、沉浸式的教育模式，通过纳入必修课程、开展校园安全实践活动、搭建线上学习平台等方式，将安全教育融入日常教学与生活，替代阶段性、突击式的宣传，让安全认知被动接收转化为主动内化。这种系统化改革，为破解传统安全教育零散、短效的痛点提供了明确方向，推动安全教育从碎片化覆盖转向系统性构建，提升教育的深度与长效性。

3.3.2. 实现网络安全教育供给侧改革的突破点

随着数字技术发展，校园网络安全风险不断迭代，而传统网络安全教育的“供给”却存在明显滞后：内容上仍聚焦“传统诈骗手段”，与学生面临的新型风险脱节；形式上仍以“文字宣传、课堂讲授”为主，难以适配大学生“数字化、互动化”的学习习惯；主体上多依赖“思政教师、辅导员”，缺乏专业技术人员参与，导致教育内容“重理论、轻实操”。大学生网络安全观培育成为推动供给侧改革的关键突破点，一方面，在教育内容上实施“精准供给”，围绕大学生高频接触的网络场景如跨境学术交流、线上兼职、社交平台互动设计教育内容，聚焦新型风险开展专项教学，确保教育供给与学生实际需求匹配；二是在教育形式上进行“创新”，如引入 VR 模拟诈骗场景、网络安全攻防实践、线上安全知识竞赛等互动式教育形式，借助数字化工具提升教育的吸引力与参与度，契合大学生的学习行为特征。除此之外，大学生网络安全观培育联合多主体经行协同，高校网信部门、计算机专业教师、公安干警等多方力量参与进行联合培育，整合理论讲解、技术实操、案例分析等多元资源，可有效弥补传统教育专业能力不足的短板。这种供给侧改革，让网络安全教育从滞后、单一转向精准、多元，大大提升教育的针对性与实效性。

3.3.3. 构建“五育并举”新型育人模式的组成部分

“五育并举”是新时代高等教育的核心育人理念，强调德育、智育、体育、美育、劳育的协同融合，而网络安全教育此前多被归为“德育”或“安全教育”的附属内容，与“五育”的融合度不足，未能充分发挥其综合育人价值。

大学生网络安全观培育作为“五育”的有机组成部分，可实现与多育的深度融合。在德育层面，培育中强调“网络空间主权”“信息伦理”“社会责任”，引导大学生树立正确的网络价值观，契合德育“立德树人”的目标；在智育层面，通过解析网络安全技术原理、开展风险检测实操，提升大学生的逻辑思维与技术应用能力，成为智育“能力培养”的延伸；在劳育层面，鼓励大学生参与校园网络安全志愿服务如安全隐患排查、新生安全指导，将安全认知转化为劳动实践，体现劳育“实践育人”的要求；在美育层面，通过引导大学生辨别网络空间中的“低俗信息”“虚假美学内容”，培养其网络审美判断力，助力美育“以美育人”；在体育层面，结合“网络沉迷对身心健康的危害”开展教育，引导大学生合理规划上网时间，间接服务于体育“健康体魄”的培育目标。这种融合价值，让大学生网络安全观培育超越“单一安全教学”的定位，成为串联“五育”、推动育人模式创新的重要纽带，助力高校实现“全人培育”的教育目标。

4. 微观维度：大学生成长成才的内在需求

4.1. 促进大学生全面发展的基础保障

数字时代下，网络已深度渗透大学生的学习科研、社交生活与职业规划，成为其成长发展的重要场域，然而，调查显示，尽管超过 80%的学生认同“维护网络信息安全是公民基本义务”，但在具体行为上却存在普遍落差。例如，超过 34%的学生表示，转发未经核实信息的主要动机是“觉得有趣”而非事实核查；在个人信息发布上，约 29%的学生会分享部分真实信息或经常“晒”包含定位、学校的动态。这深刻地揭示了从价值认同到行为自觉之间存在巨大鸿沟。网络安全观培育正是要填补这一鸿沟，通过系统的知识传授、技能训练和价值引导，将宏观的安全要求转化为大学生可理解、可执行、能坚持的日常数字行为准则，为其全面发展筑牢根基。

4.1.1. 提升数字时代生存能力的必备素养

在数字时代，大学生的学习如线上科研、跨境学术交流等，生活如社交互动、线上消费等，未来职业发展如数字化办公、网络协作等均高度依赖网络空间，而网络安全则是其在数字世界“安全生存”的前提。大学生网络安全观培育有利于帮助学生掌握数字时代必备的安全技能：从辨别可疑链接、保护个

人信息，到防范网络诈骗、规避数据泄露，再到理解网络空间主权与信息伦理，培育过程将抽象的安全认知转化为具体的生存能力。这种能力不仅能让大学生在当下校园生活中规避网络风险，更能为其未来步入社会、应对复杂数字环境奠定基础，是数字时代大学生“安身立命”的必备素养，支撑其在数字空间的自主发展与权益保障。

4.1.2. 规避网络沉迷与信息异化的防护机制

大学生网络沉迷与信息异化问题已成为当前高等教育领域亟待解决的重要课题。具体表现为部分学生无节制地沉迷于短视频、网络游戏等数字娱乐活动，以及在算法推送机制下被动接受碎片化信息并形成信息茧房。这些现象不仅对学生的学业表现和身心健康产生负面影响，更可能导致其价值认知的偏差，进而阻碍个体的全面发展。

在此背景下，加强大学生网络安全观培育不仅能够从行为层面预防网络沉迷，更能从认知层面抵御信息异化的风险，为大学生认知能力的健康发展与身心素质的全面提升提供必要保障。一方面，大学生网络安全观培育通过系统阐释网络沉迷对时间管理能力、注意力集中度及身心健康的损害机制，引导学生建立理性的网络使用意识，培养其制定科学上网计划、主动规避信息过载等自我调节能力，从而有效降低网络过度使用带来的负面影响；另一方面，大学生网络安全观培育通过提升学生的信息素养，特别是培养其对算法推荐信息的批判性思维能力和对碎片化信息的甄别能力，帮助其突破信息茧房的局限，避免陷入虚假信息和片面观点的认知陷阱，最终形成独立、理性的信息处理能力。

4.1.3. 培育健康网络心理与行为习惯的成长阶梯

在数字化生存背景下，网络心理与行为规范已成为影响大学生人格发展的重要变量。健康的网络心理体现为理性的自我认知与价值判断能力，规范的网络行为则表现为对网络伦理与法律规范的自觉遵守。这两者共同构成了大学生健全人格与道德素养的重要组成部分。大学生网络安全观培育整合了认知建构、心理调适与行为规范三重维度，形成系统化的育人机制。从心理发展角度看，培育过程有利于帮助学生克服网络虚拟性带来的认知偏差，建立稳定的网络–现实同一性认知；从道德养成维度看，则有利于促使学生将网络安全认知转化为道德自律，形成符合网络文明要求的行为范式。这不仅有助于大学生在网络环境中维持心理稳定与行为合规，更能延伸至现实生活，促进其人格完善与道德发展，最终实现心理调适、道德认知与行为规范的协同提升。

4.2. 增强网络风险应对能力的现实需要

在数字时代，线上课程学习、社交互动、网络消费、兼职求职等已成为大学生日常学习生活的重要组成部分。然而，在识别网络谣言与虚假信息方面，数据显示仅 18.27%的学生自认为“非常擅长”快速准确识别，而超过 40%的学生仅“有一定识别能力”且承认“偶尔会上当”。这凸显了提升信息甄别能力的普遍需求。在“防范个人信息泄露”方面，行为数据触目惊心：高达 43.37%的学生经常或总是使用不安全的公共 Wi-Fi，仅有 17.12%的学生每次都会仔细阅读 APP 用户协议和隐私条款。这些高风险行为的普遍存在，恰恰说明仅仅告知风险远远不够，必须通过培育使学生掌握并愿意运用具体的防护技能。因此，网络安全观培育必须超越知识灌输，致力于提供可操作的“认知工具”与“技术屏障”，切实提升大学生应对真实网络风险的能力。

4.2.1. 识别网络谣言与虚假信息的认知工具

网络世界是一个巨大的信息世界，在这个信息世界里，存在符合实际的、积极向上的信息，同时也存在着不符合实际的、消极的不良信息。而虚假信息可以借助算法推荐机制快速扩散，易导致大学生认

知偏差，甚至引发思想混乱，对其理性判断能力的培养产生不利影响。有学者指出高校网络舆情治理不仅是维护国家意识形态安全和实现国家长治久安的重要保障，也深刻影响着高校办学方向和稳定发展，更直接作用于学生的理想信念塑造、科学理性培育以及思想政治素养提升，与学生的健康成长紧密相关[11]。大学生网络安全观培育则为大学生提供识别网络谣言与虚假信息的认知工具，培育过程中通过解析网络谣言的传播逻辑即碎片化信息加煽动性内容，传授信息溯源方法如核查信息发布主体资质、交叉验证多渠道信息等方式，可以有效帮助大学生突破信息盲从的认知局限，形成“先验证、后判断”的认知习惯。这一认知工具的构建，能够有效提升大学生对网络信息的辨别能力，避免其受虚假信息误导，为其学业规划、决策制定等提供理性认知支撑。

4.2.2. 防范个人信息泄露与隐私侵犯的技术屏障

随着大学生线上活动频次的增加，其在网上娱乐、社交账号注册、兼职求职等场景中需频繁提供个人信息如姓名、手机号、身份证号等，导致个人信息暴露风险显著提升。个人信息一旦泄露，可能引发垃圾信息骚扰、身份冒用、网络诈骗等连锁危害，严重侵犯大学生的隐私权与财产权，对其个体权益造成损害。大学生网络安全培育为大学生构建防范个人信息泄露与隐私侵犯的技术屏障。在培育过程中，可以通过实操性教学，使大学生掌握具体的信息保护技术手段，如设置高强度密码、关闭应用程序不必要的权限如位置信息获取、通讯录读取权限、识别钓鱼链接如伪装成“教务通知”的恶意链接等，有效帮助大学生梳理个人隐私保护意识。同时，大学生网络安全观培育能够有效引导大学生树立个人信息分级保护意识，明确公开信息与敏感信息的界限，避免因操作不当导致个人隐私泄露。这一技术屏障的搭建，能够直接降低大学生个人信息暴露的风险，为其网络隐私安全提供切实保障，维护其合法权益不受侵害。

4.2.3. 抵御网络暴力与舆情伤害的自我保护手段

大学生在网络空间中分享生活、表达观点的行为较为普遍，但在此过程中，可能因个体言论引发恶意攻击、个人信息被恶意披露即“人肉搜索”，或因卷入小范围网络舆情，导致心理健康受损、人际关系受影响。此类网络暴力与舆情伤害不仅会引发大学生负面情绪，还可能干扰其正常的学习与生活秩序，对其个体成长产生消极影响。大学生网络安全培育可以为大学生提供抵御网络暴力与舆情伤害的自我保护手段。在教学过程中帮助大学生掌握具体的面对网络暴力与舆情伤害的应对方法，如屏蔽、拉黑恶意账号，留存相关证据并向网络平台投诉，在个人信息泄露时及时报警等，可有效帮助其走出舆论的“漩涡”，避免事态升级造成负面影响。另外，网络安全观培育注重引导大学生构建心理防护机制，如理性看待网络评价、避免因负面舆论否定自我价值，提升其心理抗压能力。这一自我保护手段的形成，能够帮助大学生在遭遇网络暴力与舆情伤害时有效止损，减少负面因素对其学习生活与心理健康的干扰，为其成长与发展保驾护航。

4.3. 培育数字时代公民责任的必然选择

网络空间作为现实社会的延伸，已成为大学生参与社会生活的重要场域。大学生在网络空间中的言论表达、信息转发、互动交流等行为，均对网络环境产生直接影响。作为未来社会建设的中坚力量，大学生在数字时代的公民责任意识，不仅关系到其个体在网络空间中的行为规范，更对网络空间秩序的维护具有重要意义，而大学生网络安全培育则有效帮助大学生从“只管好自己”变成“也能为网络做点事”，自觉成长为靠谱的“数字公民”。

4.3.1. 践行网络空间行为规范的主体自觉

网络信息传播匿名性的特点决定了网络信息的鱼龙混杂，易弱化大学生的责任感知，导致部分学生

出现发表过激言论、转发未经核实八卦信息、以“恶搞”形式调侃他人等行为失范现象。此类行为不仅可能对他人造成心理伤害与权益侵犯，更会破坏网络空间的秩序与道德生态。大学生网络安全观通过帮助大学生建构网络行为认知，可有效规范其网络行为，如通过系统解读《中华人民共和国网络安全法》等法律法规中关于网络言论、信息传播的约束条款，明确界定合法与违法、道德与失德的边界，打破大学生对“网络匿名即无责”的认知误区，让学生认识到每一项网络行为均需承担相应的法律与道德责任，从认知层面消除行为失范的潜在诱因。在此基础上，引导大学生将网络空间行为规范内化为自身行为准则，形成发言前评估、转发前核实的行为习惯，在网络空间中坚守道德与法律底线，成为网络秩序的维护者而非破坏者。

4.3.2. 参与网络空间治理的社会责任担当

网络空间治理不是“你方唱罢我登场”的独角戏，而是多元主体共同参与的系统工程，大学生作为网络社会中最活跃的主体，其参与度直接影响网络治理效能。大学生网络安全培育可有效强化大学生参与网络空间治理的社会责任担当，培育过程中，可通过案例教学如展示大学生参与网络辟谣、组织校园网络志愿服务活动如协助排查迎新社群中的可疑账号、开展校园网络安全知识宣讲等方式，引导大学生认识到自身在网络空间治理中的主体地位与作用，激发其主动参与网络空间建设的意愿。这一社会责任担当的培育，不仅有助于提升校园网络治理水平、营造清朗的校园网络环境，更能推动大学生在实践中提升社会责任感，为网络空间治理注入“青春力量”，实现大学生“个体成长”与“社会贡献”的统一。

5. 总结

综上所述，新时代大学生网络安全观培育绝非孤立的教育环节，而是贯通国家总体安全战略、高等教育现代化使命与个体成长成才需求的关键纽带。从筑牢国家网络空间安全屏障，到丰富“大思政”育人格局、推动安全教育体系创新，再到赋能大学生提升数字生存能力、践行网络公民责任，其价值已超越单一的风险防范范畴，成为支撑民族复兴、适配数字中国建设的基础性工程。

面向未来，网络空间的复杂性与不确定性将持续升级，大学生网络安全观培育的深度与广度也需随之拓展。唯有充分认知其多重价值意蕴，将培育工作融入教育教学、校园治理与社会实践的全过程，才能真正让大学生成长为网络安全的坚定守护者、网络空间的积极建设者，为构建安全、健康、有序的网络生态，实现国家网络强国目标注入持久且强劲的青春力量。

基金项目

南昌航空大学研究生创新专项资金项目校级项目 YC2024-111：高校意识形态教育研究的回顾与展望——基于 Citespace 可视化分析。

参考文献

[1] 中央网络安全和信息化委员会办公室. 习近平总书记关于网络强国的重要思想概论[M]. 北京: 人民出版社, 2023: 85.

[2] 联合国教科文组织. 全球媒介与信息素养评估框架: 国家状况与能力[M]. 张开, 耿益群, 译. 北京: 中国传媒大学出版社, 2022: 55.

[3] Kellner, D. and Share, J. (2007) Critical Media Literacy: Crucial Policy Choices for a Twenty-First-Century Democracy. *Policy Futures in Education*, **5**, 59-69. https://doi.org/10.2304/pfie.2007.5.1.59

[4] 周宗奎. 网络心理学[M]. 上海: 华东师范大学出版社, 2017: 121-123.

[5] Kovačević, A., Putnik, N. and Tošković, O. (2020) Factors Related to Cybersecurity Behavior. *IEEE Access*, **8**, 125140-125148. https://doi.org/10.1109/access.2020.3007867

[6] 赵春欢. 社会转型期我国意识形态安全风险预警研究[M]. 北京: 人民出版社, 2020: 164.

[7] 刘章仪. 青少年数字素养培育: 内容体系、多维价值与实践进路[J]. 中国广播电视学刊, 2024(2): 20-24.
[8] 郭强, 刘晓研. 新时代网络意识形态治理: 问题与对策[J]. 理论探讨, 2023(3): 99-104.
[9] 习近平谈治国理政[M]. 北京: 人民出版社, 2014: 198.
[10] 陶建杰, 李彤. 校园媒体对高校网络舆情的引导优势与实施策略[J]. 思想理论教育, 2017(1): 82-85.
[11] 刘鸿滨, 孙海清. 新时代高校网络舆情治理的风险审视和路径拓新[J]. 学校党建与思想教育, 2025(15): 86-89.