

College Students' Network Literacy Education in the Omnimedia Era: Value, Content and Path

Tao Jiang, Jiying Zhao*

School of Marxism, Northeast Agricultural University, Harbin, Heilongjiang, China

**Corresponding Author*

Abstract: In the omnimedia era, the Internet is an important field for college students to learn, live, communicate, and entertain, and it is also an important position for college ideological and political work teams to carry out ideological and political education for college students. College students need to have good network literacy in the process of surfing the Internet. Carrying out network literacy education has become the consensus of the ideological and political work teams in colleges and universities. Continuously improving the network literacy of college students is to meet the needs of college students' healthy growth, meet the need to cultivate new people in the era, and build a network of power. The ideological and political work team in colleges and universities needs to strengthen college students' network cognitive education, network behavior, ability education, and network emotion and value education. To strengthen the network literacy education of college students, it is necessary to give full play to the leading role of the government, strengthen the main role of colleges and universities, effectively play the auxiliary role of society, and give full play to the subjective initiative of college students.

Keywords: Omnimedia Era; College Students; Network Literacy Education; Content; Path

1. Introduction

In the omnimedia era, digital networks have become an indispensable medium for university students to retrieve information, acquire knowledge, and engage in interpersonal communication, presenting a critical pedagogical challenge regarding how to cultivate students' digital competence to foster holistic personality development, facilitate healthy growth, and ultimately nurture talents

who can contribute meaningfully to societal progress—a dual imperative constituting both a reflective exercise for students and an institutional responsibility for higher education establishments that must prioritize network literacy education as a core component of comprehensive competency cultivation to address the developmental needs of contemporary undergraduates, wherein we conceptualize university students' network literacy as a multidimensional construct encompassing cognitive understanding of networked ecosystems, operational proficiency in utilizing connected devices and platforms through various applications, critical capabilities in information acquisition, discernment, creation, and dissemination, self-protection awareness in cyberspace, and ultimately the developmental capacity to leverage digital resources for personal and professional growth.

2. The Value Implications of Enhancing University Students' Network Literacy

As a crucial domain for learning, daily life, social interaction, and entertainment, the digital space has also become an important front for ideological and political education in higher institutions. The appropriate use of online platforms, responsible dissemination of information, active yet discerning participation in digital life, and the cultivation of a healthy cyberspace all necessitate advanced network literacy. Integrating network literacy education into ideological and political education is therefore imperative for universities—not only to meet students' developmental needs but also to align with China's strategic vision of building a cyber superpower.

2.1 The Imperative of Enhancing Network Literacy for University Students' Healthy Development

As authentic "digital natives," contemporary

university students exist in a state of perpetual connectivity where internet engagement has become ubiquitous across all temporal and spatial dimensions of their lives, constituting a fundamental element in their developmental trajectory that presents both transformative opportunities and substantial challenges. While digital platforms serve as indispensable conduits for knowledge acquisition and personal growth, they simultaneously expose students to multifaceted risks including internet addiction disorder, information anxiety syndrome, digital stress, and privacy vulnerabilities, with empirical evidence revealing pervasive "digital dependency" behaviors manifested through compulsive engagement with Weibo during transit, Douyin while dining, Xiaohongshu before sleep, Bilibili during class intervals, and even Honor of Kings gameplay during instructional periods, reflecting a concerning pattern of excessive digital immersion. The heterogeneous quality of online information, where credible content coexists with misinformation, exacerbates these challenges as many students demonstrate insufficient critical literacy competencies to effectively identify, evaluate, and utilize digital information, resulting in clinically observable information anxiety, while the proliferation of detrimental content promoting materialistic display, hedonistic pursuits, and sensationalist narratives (encompassing sexual, violent, and scandalous material) further compounds these issues by distorting value orientation and decision-making processes. In the post-Xiaokang era, as students pursue enhanced developmental aspirations, higher education institutions must implement comprehensive network literacy education programs designed to cultivate responsible digital citizenship through (a) establishing normative online conduct frameworks, (b) enhancing information discernment and ethical dissemination capacities, (c) strengthening privacy protection mechanisms, (d) mediating virtual-real life integration, and (e) fostering resilient digital identities, thereby enabling students to navigate omnimedia environments while developing the multifaceted competencies required for holistic personal and professional development in alignment with national strategic priorities for human capital cultivation in the digital age.

2.2 Enhancing University Students' Network

Literacy: A Foundational Element for Building a Cyber Superpower

In the omnimedia era, the transformative power of digital networks has become increasingly prominent, serving not only as a potent engine for socioeconomic transformation but also as a critical driver for enhancing comprehensive national strength, with China having strategically implemented pivotal initiatives including the Digital China strategy, the National Big Data Strategy, and the "Internet Plus" Action Plan to accelerate its modernization process, where the realization of these national digital ambitions requires both cutting-edge network technologies and a citizenry possessing sophisticated network literacy competencies, making it imperative for higher education institutions to systematically cultivate students' digital proficiency to produce qualified netizens who can meet these strategic demands, as evidenced by the fact that students with well-developed digital ethics consciously engage in civilized online behaviors by actively resisting vulgar, kitsch, and lowbrow content while refraining from disseminating violent or pornographic material, and those possessing refined digital etiquette demonstrate prudence, authenticity, and respect for privacy in virtual interactions while abstaining from rumor creation, belief, or propagation, with such cultivated competencies directly contributing to two fundamental pillars of digital nation-building - robust cybersecurity and healthy digital ecosystems, particularly crucial given China's current status as a global internet power where cyberspace has shown continuous improvement in clarity and positive ecological development [1], yet still faces challenges from disruptive noises and harmful discourses that necessitate persistent efforts to maintain pristine cyberspace conditions [2], wherein university-based network literacy education emerges as a vital mechanism for empowering students to become active agents in ecological improvement by consciously safeguarding network security, combating uncivilized behaviors like rumor-mongering, and opposing illegal activities threatening national cyber safety, thereby collectively fostering the wholesome digital environment essential for achieving China's aspirations of digital preeminence.

3. The Composition of Network Literacy

Education

Network literacy education encompasses, beyond fundamental network cognition instruction, two primary domains: network behavior and competency development, as well as digital affect and value cultivation, constituting an integrated framework that addresses both the technical and socio-ethical dimensions of online engagement to foster comprehensive digital citizenship in higher education contexts.

3.1 Network Behavior and Competency Education

Network behavior and competencies refer to university students' practical operational activities in digital environments and their corresponding capabilities to effectively execute these activities, wherein higher education institutions play a pivotal role in cultivating network literacy by not only guiding students to regulate their online conduct in accordance with established norms but also enhancing their capacity to utilize digital resources in a lawful and appropriate manner, thereby fostering responsible digital citizenship that aligns with both personal development goals and societal expectations in the information age.

3.1.1 Information discernment competency in digital environments

In contemporary digital ecosystems where platforms such as Weibo, Douyin, Bilibili, Toutiao, and various online forums constantly inundate users with an overwhelming deluge of heterogeneous information, university students risk becoming cognitively disoriented in this vast informational ocean without robust information discernment capabilities. Higher education institutions must prioritize the cultivation of critical network literacy through ideological and political education initiatives that empower students to maintain independent thinking and exercise rational judgment while navigating online spaces. The digital information landscape presents multifaceted authenticity challenges, including: (a) information distortion due to non-objective reporting, (b) message alteration during viral dissemination processes, and (c) deliberate fabrication by malicious actors. Pedagogical interventions should strategically guide students to: (i) prioritize authoritative sources (e.g., People's Daily Online, Guangming Online, and

official government platforms) for credible information, (ii) employ multi-source verification protocols when encountering content from unofficial channels particularly self-media accounts, and (iii) develop systematic skepticism towards unverified claims. Furthermore, the pervasive existence of sensationalized content encompassing sexual, violent, and provocative material necessitates that educators facilitate critical analysis of both the negative societal impacts and underlying production mechanisms of such content, while simultaneously fostering dialectical thinking skills that enable students to reach substantiated conclusions through reflective inquiry and evidence-based evaluation processes.

3.1.2 Digital political participation competency
Digital political participation competency constitutes the multidimensional capacity of netizens to exercise oversight over governmental institutions, articulate legitimate interest appeals through research reports, policy proposals, or other formal channels, and exert constructive influence on political decision-making processes, a capability that has gained increasing significance in China's new era characterized by accelerated democratic political development and the substantive implementation of whole-process people's democracy, where heightened political engagement among citizens—particularly university students—has manifested through growing utilization of digital platforms to supervise governmental operations and voice reasonable demands, necessitating that ideological and political educators in higher education institutions innovate pedagogical approaches by cultivating students' normative frameworks for digital political engagement through (a) fostering legally-compliant and orderly participation mindsets, (b) developing practical competencies via simulated policy-making activities such as "Model Proposal Competitions," and (c) encouraging micro-level civic engagement that transforms local observations into actionable policy recommendations, with empirical evidence demonstrating that politically-active students not only enhance their political consciousness, ideological steadfastness, and governance literacy but also accelerate political socialization processes while contributing to governance system optimization through (i) providing intellectual support to public

administration and (ii) forming a talent pipeline for civil service, thereby creating synergistic value that simultaneously advances individual civic development and national governance modernization objectives within the digital transformation of China's political ecosystem.

3.1.3 Competency in countering malicious online speech and conduct

The internet serves as a convergence point for diverse discourses, public sentiments, and ideological trends, constituting a contested space where ideological struggles manifest with particular acuity and complexity, thereby necessitating systematic efforts by higher education institutions to enhance students' capacity to identify and resist harmful online behaviors and rhetoric through targeted network literacy education that elucidates the challenges confronting dominant ideologies in cyberspace. Contemporary digital environments exhibit a pronounced tendency toward pan-entertainment, which exerts deleterious effects on mainstream ideological frameworks, as evidenced by instances where netizens—motivated by the "attention economy" paradigm and the problematic "traffic-first" mentality—engage in historical distortion, heroic figure mockery, revolutionary martyr defamation, as well as the propagation of money worship and nihilism, all of which pose significant ideological challenges. Concurrently, Western nations leverage their technological and cultural hegemony to perpetuate ideological infiltration through digital channels, promoting erroneous conceptions such as liberal democracy and capitalist values while advancing theories of "China threat," circumstances that demand universities cultivate students' abilities to critically analyze the underlying nature of these phenomena, develop conscious resistance strategies, and engage in principled opposition through well-reasoned, evidence-based refutations that maintain decorum while demonstrating ideological steadfastness, with particularly egregious cases requiring formal reporting to platform administrators or relevant government authorities as part of collective efforts to preserve the integrity and clarity of cyberspace.

3.2 Cyber Values and Affect Education

Cyber Values and Affect refer to the normative value frameworks and emotionally healthy, positive dispositions that university students

must cultivate when engaging with cyber environments. In implementing cyber literacy education, ideological and political educators in higher education institutions are required to (a) systematically deliver cyber-ethical value instruction, (b) facilitate the internalization of appropriate online value systems, and (c) nurture constructive emotional responses to digital interactions, thereby enabling students to establish correct cyber-ethical orientations while developing psychologically resilient and upwardly aspirational affective states in their online engagements.

3.2.1 Cyber legal literacy education

Cyber legal literacy represents an integrated competency encompassing knowledge-based, theoretical, normative, and behavioral dimensions centered on the core value of rule of law [3], recognizing that while cyberspace may be virtual, its users exist in reality and must adhere to legal frameworks, necessitating that higher education institutions embed legal consciousness and jurisprudential thinking throughout network literacy curricula in alignment with the comprehensive rule of law strategy, through which students develop (a) enhanced sensitivity to legal/illegal online behaviors via study of cybersecurity legislation and related regulations, (b) understanding of boundaries for free speech that preclude dissemination of sensationalized or harmful content while actively maintaining digital order, (c) comprehension of intellectual property rights including open-source and creative commons principles to prevent infringement, (d) capacity for personal and collective privacy protection, (e) commitment to digital integrity by rejecting rumor propagation and false representation, and (f) resilience against cyberbullying through empowered resistance to online violence and harassment—collectively fostering a harmonious cyber ecosystem where students additionally learn to navigate cyberspace's dual role as both public opinion forum and amplification mechanism, enabling their constructive participation in guiding online discourse toward positive value dissemination, with such comprehensive legal literacy cultivation serving to intrinsically motivate students' engagement with cyber jurisprudence while clarifying its societal significance [4], ultimately empowering them to safeguard personal and collective legal rights, maintain cyberspace order, and ensure the

internet's development within proper legal parameters.

3.2.2 Cyberspace sovereignty awareness education

Cyberspace sovereignty refers to the jurisdiction a state exercises over information communication technology activities and systems, as well as the data they carry, within the cyberspace located within its territory [5]. The awareness of cyberspace sovereignty denotes a nation's or region's understanding of its autonomy, independence, and control over its activities and systems in cyberspace. By strengthening education on the awareness of cyberspace sovereignty, universities can enable students to acquire and master relevant knowledge regarding cyberspace sovereignty. In the early stages of internet development, scholars and internet professionals such as David Johnson and David Post argued that the internet was a free space, unconstrained by the legal rules of the real world. This view was also supported by John Barlow, founder of the Electronic Frontier Foundation (EFF), through his influential "Declaration of Independence of Cyberspace". However, later, Professor Timothy Wu, an American scholar, proposed the concept of "cyberspace sovereignty," arguing that cyberspace possesses sovereign attributes and that real-world legal principles apply to it [6]. With the evolution of cyber practices, the persistent emergence of illicit activities such as online fraud and pornography has prompted the international community to increasingly prioritize cyberspace governance, leading to broader recognition of cyberspace sovereignty among nations and international organizations, as evidenced by the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, which formally acknowledges cyberspace sovereignty by categorizing it into "internal sovereignty" and "external sovereignty" while delineating its scope to encompass both cyber activities and infrastructure [7]—a conceptual framework that aligns with China's legislative intent in promulgating the Cybersecurity Law to safeguard national cyberspace sovereignty, wherein higher education institutions play a pivotal role in cultivating students' sovereignty awareness through systematic education that enables them to (a) comprehend the strategic significance of cyberspace sovereignty within contemporary geopolitical contexts, (b) identify

behaviors that infringe upon national digital sovereignty during online activities, and (c) develop the capacity and courage to counteract unlawful actions, thereby contributing to the collective effort of preserving sovereign integrity in digital domains through informed civic participation and vigilant oversight.

3.2.3 Cyber ethical literacy education

Cyber ethical literacy encompasses the moral principles and behavioral norms that individuals should adhere to when engaging in online activities, representing a critical extension of personal morality into the digital realm [8], wherein while university students typically demonstrate compliance with ethical standards in physical social interactions, the anonymity and detachment characteristic of virtual environments may lead to ethical complacency or even abandonment of moral constraints, resulting in problematic online behaviors, thus necessitating that higher education institutions strengthen cyber ethics education through (a) systematic cultivation of cyber-ethics and online civility, (b) integration of traditional cultural virtues, national spirit, contemporary values, and exemplary models into curriculum design [9], and (c) practical guidance for students to uphold ethical principles in cyber spaces through respecting others, offering assistance, and practicing "ethical solitude" (shen du) - a Confucian-derived concept of self-discipline requiring conscious avoidance of violent or pornographic content, refraining from disseminating vulgar materials, abstaining from doxxing or privacy violations, rejecting misinformation propagation, and strictly observing both legal regulations and the National Youth Cyber Civilization Convention, while also encouraging proactive ethical engagement through participation in online philanthropic activities and provision of assistance to those in need within legal boundaries, thereby collectively fostering a wholesome cyber ecosystem that promotes the healthy development of cyberspace through the synergistic combination of moral restraint and active civic virtue.

3.2.4 Cybersecurity literacy education

Cybersecurity literacy represents a multidimensional competency encompassing university students' knowledge of cybersecurity principles, awareness of digital threats, and practical skills to address security challenges in legally compliant manners, with the internet

having evolved into a virtual habitat for modern life where, analogous to physical society, various risks necessitate global attention to cybersecurity issues—a concern addressed through enhanced cybersecurity literacy as demonstrated by Western nations such as the United States, United Kingdom, and Australia incorporating cybersecurity education into national development strategies and legal frameworks, mirroring China's progressive integration of cybersecurity awareness into key policy documents including the National Cyberspace Security Strategy and Cybersecurity Law, wherein higher education institutions must implement comprehensive cybersecurity literacy programs through collaborative efforts between ideological-political educators and technical specialists to cultivate students' (a) appreciation for cybersecurity significance, (b) mastery of protective knowledge and techniques, (c) adoption of normative cybersecurity perspectives, (d) disciplined online conduct emphasizing privacy protection and credential management, (e) compliance with ethical and legal standards, and (f) critical discernment capabilities, while additionally fostering vigilance against cyber activities threatening national security through proper reporting channels, ultimately transforming students into proactive advocates and practitioners of cybersecurity who contribute to both individual protection and national digital defense systems through their daily online practices and security consciousness.

4. Pathways for Enhancing University Students' Network Literacy in the Omnimedia Era

In the omnimedia era, digital networks have become increasingly indispensable in propelling societal advancement, with their pervasive integration across all domains of human activity rendering them fundamentally inseparable from contemporary civilization, a reality that necessitates elevated network literacy among university students as key agents of China's social development—where comprehensive enhancement of such literacy constitutes both an essential component in implementing the national strategy for digital empowerment and a critical safeguard for students' holistic development, requiring synergistic collaboration among governmental entities,

higher education institutions, societal stakeholders, and students themselves to establish an integrated ecosystem that fosters multi-dimensional cyber competency development through policy formulation, curricular innovation, cultural cultivation, and self-directed learning initiatives aligned with the demands of digital transformation in the new era.

4.1 Maximizing Government's Leadership Role in Network Literacy Education

Within the framework of university students' network literacy cultivation, the government assumes an irreplaceable leadership position that transcends the capacities of both higher education institutions and societal actors, wielding unique administrative authority to implement top-down strategic planning through (a) systematic integration of network literacy objectives into national development blueprints, (b) formulation and refinement of pertinent legal regulations and policy instruments, and (c) active cultivation of a wholesome and ethically-grounded cyber ecosystem, thereby exercising comprehensive governance across policy-making, legislative oversight, and cultural shaping dimensions to establish an enabling environment that coordinates multi-stakeholder efforts while ensuring alignment with national strategic priorities in digital transformation and human capital development.

4.1.1 Formulating network literacy education Plans

Western nations such as the United States and the United Kingdom have long incorporated network literacy education into their national development strategies, with the U.S. enacting comprehensive frameworks including the Comprehensive National Cybersecurity Initiative, National Cybersecurity Education Strategy, and National Cybersecurity Strategy to emphasize cybersecurity awareness across all demographics, while the UK has issued policy documents such as Commonwealth Cyber Capacity Building Programme (2018-2021), National Cyber Strategy 2022, and National Cyber Security Strategy 2022-2030, which prioritize the establishment of academic centers of excellence in cybersecurity education and research to enhance public digital competencies and cyber resilience. In contrast, while China has referenced network literacy education in key policy documents—such as the Medium-

and Long-Term Youth Development Plan (2016–2025) advocating for "scientific, legal, civilized, and rational internet use among youth," the Ministry of Education's 2019 Work Priorities calling for "strengthening university students' network literacy education," and the Department of Ideological and Political Affairs' 2021 Work Priorities proposing "a training system for improving students' network literacy and instructors' online ideological education capabilities"—these mentions remain cursory, lacking detailed implementation guidelines, safeguard mechanisms, or promotion strategies. To address this gap, the Chinese government should draw upon successful Western models by aligning network literacy education with the national Cyberpower Strategy and leveraging education, technology, and talent development initiatives to establish a comprehensive framework, including the formulation and implementation of Guidelines for Network Literacy in Higher Education and University Students' Network Literacy Standards, thereby systematically enhancing students' digital competencies, fostering holistic development, and cultivating a new generation of highly capable individuals equipped for the digital age[10].

4.1.2 Strengthening cyber governance through legal frameworks

The healthy and orderly development of the internet necessitates robust legal safeguards, requiring comprehensive governance through legal oversight of cyberspace, lawful operation of online platforms, and legal compliance in internet usage to ensure the digital ecosystem operates within juridical parameters, where the cultivation of university students' network literacy fundamentally depends on governmental regulatory enforcement and legal administration of cyberspace, as institutionalized through China's constitutional and legal framework including the National Security Law, Cybersecurity Law, Internet Information Service Management Measures, and Regulations on the Ecological Governance of Online Content, which collectively establish the normative foundations for cyber governance; governmental agencies must continually refine this legal architecture by modifying, supplementing, and perfecting cyber legislation in accordance with the ontological characteristics of digital space and operational logics of network systems, precisely delineating

the rights and obligations of cyber actors to achieve rule-of-law governance that fosters a wholesome online environment [11], with specific enforcement measures requiring: (a) stringent legal sanctions by state security and public security organs against activities endangering national security, rumor-mongering entities, and illegal operations involving pornography, gambling, or drugs, coupled with university-collaborated "case-based legal education" initiatives to reinforce students' understanding of legal boundaries in digital spaces; (b) prompt intervention by cyberspace authorities against sensationalized content promoting materialism, hedonism, or other values, balanced with proactive creation of appealing, people-affirming media content that meets student needs while amplifying mainstream ideologies; and (c) targeted campaigns against self-media misconduct, internet trolls, and misinformation through enhanced professional certification for content creators, optimized review mechanisms, and advanced detection of duplicated malicious content to prevent "bad money driving out good" scenarios in digital content production, thereby guiding students toward lawful and civilized internet engagement as exemplary "Chinese Good Netizens" who collectively contribute to cultivating a clean cyberspace and fostering a healthy digital ecosystem.

4.2 Strengthening the Central Role of Higher Education Institutions

As the primary institutional setting for university students' academic and daily life, higher education establishments possess unique advantages in enhancing network literacy and must therefore assume principal responsibility by leveraging their pivotal position as key educational platforms, which can be operationalized through systematic development and refinement of network literacy curricula alongside the implementation of practical educational initiatives designed to cultivate comprehensive online competencies.

4.2.1 Improving the curriculum system for network literacy education

The classroom is the primary channel for education, and curricula are a reliable foundation for educational implementation. In conducting network literacy education for university students, higher education institutions should guide their efforts with the

concept of "ideological and political education integrated into curriculum" (Ke cheng si zheng), organically integrating network literacy education into various courses to establish a comprehensive and well-structured curriculum system for network literacy. Firstly, integrating network literacy education into ideological and political theory courses. As a compulsory course for university students, ideological and political education has broad coverage. In the "Principles" course, teachers can guide students to analyze phenomena in cyberspace using dialectics, helping them understand the essence of issues beyond superficial appearances. In the "Introduction to New Thought" course, teachers should encourage students to maintain a correct online public opinion orientation, uphold cultural confidence, strengthen their awareness of cybersecurity, act as responsible gatekeepers, and promote positive energy. In the "Ideological and Legal Foundations" course, teachers should integrate online ethics and legal knowledge into their teaching, guiding students to practice self-discipline and cultivate mainstream values and a strong sense of cybersecurity awareness [12]. In the "Outline of Modern Chinese History" course, teachers can use online events such as the denial of "Huang Jiguang blocking the bullet" to analyze the dangers of historical nihilism, guiding students to firmly believe in the confidence of history. Secondly, leveraging fundamental computer science courses as a platform for network literacy education enables students to acquire essential technical competencies including computer and network fundamentals, cybersecurity principles, database technologies, and computational thinking, along with practical skills in operating systems and office productivity software (e.g., WPS Office), while thirdly, the establishment and enhancement of dedicated network literacy curricula - either through institutionally-developed courses or by incorporating high-quality MOOCs such as Sun Yat-sen University's "New Media Literacy" and Beijing Institute of Technology's "Enhancing University Students' Media Literacy" - provides structured learning opportunities for students to develop advanced capabilities in information retrieval, critical evaluation of online content (including identification of sensationalized or inappropriate material), and responsible digital citizenship, thereby creating a comprehensive pedagogical ecosystem that combines technical

proficiency with critical media literacy through both existing course adaptations and specialized program development.

4.2.2 Implementing diverse network literacy education initiatives and practical activities

Practical activities in network literacy education serve as a vital pathway for enhancing university students' online competencies, with an increasing number of higher education institutions organizing comprehensive programs that effectively integrate classroom instruction with experiential learning through two primary approaches: firstly, by facilitating student participation in government-led initiatives such as those administered by "China University Students Online" - the Ministry of Education's flagship platform for ideological and political education - which has conducted specialized programs including "University Students' Network Literacy Training Workshops," "Network Literacy Enhancement Lectures," and "University Cyber Culture Festivals," with institutions like Zhejiang Ocean University and Sichuan Institute of Industrial Technology actively engaging their students in these activities that combine instructional videos, expert lectures, and hands-on practice, culminating in certified e-learning credentials upon successful completion, while provincial and municipal authorities have concurrently launched campaigns such as "Model Cyber Citizens on Campus" and "My Contribution to Cyber Civility" to encourage positive online engagement; secondly, through institutionally-designed programs where universities systematically consolidate and optimize existing activities to develop premium network literacy projects [13], exemplified by initiatives like "Network Literacy Enhancement Bootcamps" and "Mind Your Digital Words and Deeds" that cultivate students' awareness, cognitive understanding, operational skills, and behavioral discipline in cyberspace, with resource-endowed institutions further establishing "Cyber Civility Education Practice Bases" and "Network Literacy Demonstration Centers" as dedicated platforms for advancing cybersecurity awareness, protective skills, and the propagation of positive online discourse, thereby creating a multidimensional ecosystem for digital citizenship cultivation.

4.3 Effectively Leveraging Societal Support Mechanisms

Higher education institutions exist neither as isolated ivory towers nor utopian enclaves, but rather as integral components of broader social ecosystems wherein students' network literacy development is inevitably shaped by societal influences, making the cultivation of a constructive social environment paramount for fostering accurate cyber-cognition, nurturing disciplined online behaviors, and enhancing comprehensive digital competencies that collectively contribute to students' holistic growth and professional preparedness in the digital era.

4.3.1 Strengthening accountability of digital platforms

As both the primary arena for online activities and service providers, digital platforms must rigorously fulfill their primary responsibilities by implementing concrete measures to enhance university students' network literacy through three key dimensions: firstly, intensifying network literacy education initiatives by developing comprehensive educational plans that leverage their professional expertise and influence to establish dedicated network literacy columns, disseminate cybersecurity knowledge, promote internet-related laws and regulations, propagate anti-fraud techniques, and advocate for civilized online behavior; secondly, conscientiously executing their "gatekeeping" functions through strict compliance with legal frameworks, including implementing robust content review mechanisms for published information with particular attention to value orientation, conducting regular self-audits using both technological and manual methods to identify and address problematic content, promptly remove posts, blog articles and short videos that violate national regulations, suspending accounts that persistently distribute vulgar or sensationalized content, and reporting accounts publishing illegal information (such as those defaming heroes or undermining state authority) to public security and state security organs, while simultaneously enhancing social responsibility awareness to better manage entertainment content, prevent excessive entertainment tendencies, and provide proper guidance to prevent students from falling into ideological pitfalls like consumerism and hedonism; thirdly, rigorously enforcing real-name registration systems that effectively curb malicious content by mandating backend

authentication for all registered accounts and implementing front-facing real-name verification for influential self-media accounts, a dual-layered identification system that not only regulates online behavior of public figures to set positive examples for students but also significantly contributes to cultivating a wholesome cyberspace ecosystem.

4.3.2 Enhancing self-regulation in the self-media industry

The omnimedia era has transformed every individual into both a consumer and producer of information, wherein the vast proliferation of self-media platforms wields substantial influence that significantly impacts university students' network literacy development, necessitating rigorous self-discipline within the self-media industry to ensure all online activities comply with national laws, regulations, and social morality through three critical dimensions: firstly, the self-media industry must strengthen sectoral self-regulation by adhering to the Notice on Strengthening Self-Media Management issued by the Cyberspace Administration of China, which outlines thirteen regulatory measures including stringent prevention of impersonation and enhanced handling of typical violation cases, while complying with various regional self-disciplinary conventions such as the Chizhou Self-Media Industry Self-Regulation Convention and the Capital Internet Platform Self-Media Management Convention, all of which require maintaining correct political orientation, disseminating mainstream ideologies, participating in cyber civilization construction, promoting traditional virtues, resisting online rumors, abstaining from illegal online publicity activities, and voluntarily accepting public supervision; secondly, influential online figures including key opinion leaders (KOLs) and live-streaming celebrities—who possess millions of followers and can trigger exponential information dissemination through multi-level sharing—must exercise exceptional prudence in their online discourse, basing all statements on verified facts without exaggeration, minimization, or distortion, and strictly avoiding sensationalized or false content for traffic acquisition; thirdly, ordinary self-media practitioners, while lacking massive followings, must equally enhance self-regulatory awareness by producing authentic, positive content that contributes to a wholesome

digital environment conducive to students' literacy development, rather than pursuing traffic and followers through morally-questionable means.

4.4 Harnessing Students' Subjective Initiative in Network Literacy Development

As external factors invariably operate through internal determinants, the concerted efforts of government, higher education institutions, and society at large - all constituting external influences relative to university students - must ultimately catalyze students' intrinsic motivation, necessitating that educational strategies prioritize the activation of learners' autonomous agency by cultivating self-directed learning competencies that enable students to internalize network literacy principles through reflective practice, critical self-assessment, and proactive skill acquisition, thereby transforming passive knowledge reception into active capability construction within personalized learning trajectories that align with their developmental needs in the digital era.

4.4.1 Cultivating university students' awareness of network literacy enhancement

Through systematic network literacy curricula, university students acquire foundational network knowledge and develop an acute awareness of both the pivotal role of cyberspace in the omnimedia era and the critical importance of digital competencies, thereby progressively strengthening their consciousness of literacy improvement by (a) diligently mastering technical operational skills during instructional sessions, (b) internalizing cyber legislation to establish law-abiding mindsets, (c) advancing personal cyber-ethics through enhanced moral cognition and judgment capacities that manifest in civilized and authentic online behaviors, (d) fostering sovereignty awareness to identify and resist "color revolution" attempts while safeguarding ideological and national cybersecurity, and (e) developing scientific thinking abilities to discern information quality, effectively liberating themselves from "information cocoons" and transcending "information isolation"; moreover, students should proactively participate in network literacy initiatives including "Internet Plus" technology festivals, cybersecurity awareness campaigns, university cyber culture festivals, and network literacy bootcamps, constituting a

comprehensive self-improvement paradigm that synergizes formal education with practical engagement to achieve holistic competency development in the digital domain [14].

4.4.2 Self-regulation of online conduct among university students

Despite its virtual nature, cyberspace remains subject to the moral codes and legal frameworks of physical society, necessitating that university students internalize the principle that "the internet is not a lawless domain" and consciously align their online behaviors with ethical and juridical standards by (a) abstaining from pornographic and violent content to cultivate refined personal tastes, (b) actively participating in digital philanthropy such as the "University Students Cyber Civility Volunteer Initiative" to elevate moral consciousness, (c) enhancing information security awareness through protection of personal and others' privacy while identifying telecommunications fraud and phishing attempts, (d) strengthening cybersecurity vigilance to detect and report espionage activities to state security authorities, and (e) developing ideological security discernment to resist non-Marxist and pseudo-Marxist rhetoric; furthermore, students must rigorously adhere to the National Youth Cyber Civility Convention and New Era Youth Cyber Civility Convention by refraining from disseminating content detrimental to national, ethnic, or social security, avoiding vulgar and sensational materials, abstaining from cyberbullying, proactively sharing China's positive narratives, and exemplifying model digital citizenship—thereby collectively fostering a wholesome online ecosystem that contributes to national cyberpower development through progressive enhancement of their digital competencies.

5. Conclusion

In the omnimedia era, the internet has become an indispensable force shaping university students' academic and personal development, with the evolving digital landscape necessitating advanced network literacy competencies that now constitute a critical factor in building China's cyberpower; higher education institutions play a pivotal role in this transformative process by implementing comprehensive network literacy education programs that not only enhance students' online capabilities but also construct a vital bridge for

their successful navigation of the digital age, cultivating them to become ethical stewards of cyberspace while simultaneously contributing to the creation of a well-regulated, harmonious online ecosystem governed by the rule of law and characterized by intellectual clarity, thereby achieving the dual objectives of individual empowerment and national digital advancement through systematic pedagogical interventions that align with the strategic demands of the new media environment.

Acknowledgments

This work was supported by the National Social Science Fund of China titled "Research on the Dissemination Mechanism and Governance Strategies of Network Ideology Based on Complex Heterogeneous Graph Structures" (No.22BXW052).

References

- [1] Xiang Z, Deng C D. The Logical Connotation of Cyberspace Governance from the Perspective of Chinese-style Modernization. *Journal of North University of China (Social Science Edition)*, 2025, 41(02):28-36.
- [2] Zhang Y J. Strengthening Cyber Ecology Governance to Create a Clean Cyberspace. *China Cyberspace*, 2025(07): 18-21.
- [3] Wu D C, Ni H. Research on Improving College Students' Digital Legal Literacy in the Digital Age. *Journal of Henan Open University*, 2024, 37(03): 108-112.
- [4] Zhang H X. The Value and Pathways of Enhancing College Students' Digital Legal Literacy in the New Era. *Guangxi Youth Development Studies*, 2025, 35(02): 26-30+58.
- [5] Fang B X. *On Cyberspace Sovereignty*. Science Press, 2017.
- [6] Timothy S. Wu, *Cyberspace Sovereignty: The Internet and the International System*. Harvard Journal of Law & Technology, 1997(3): 647-666.
- [7] Zhang Z Y. Research on State Responsibility Attribution Mechanisms in Cyber Attacks: Using the Tallinn Manual 2.0 as Reference. *Journal of Lanzhou University of Arts and Science (Social Sciences Edition)*, 2025, 41(04): 94-102.
- [8] Ji H, Wang Y M, Xu Q. Pathways to Enhance University Students' Digital Ethical Literacy. *Western Quality Education*, 2023, 9(16): 18-21.
- [9] Zhou Lijun. Analysis on Strengthening University Students' Digital Ethics Education. *Journal of Social Science of Jiamusi University*, 2023, 41(04):128-130.
- [10] Ning N X. Research on the Content, Carriers, and Mechanisms of Network Literacy Education for College Students in the New Era. *Modern Vocational Education*, 2024(30):13-16.
- [11] Xu X L, Ju H Y, Teng J C, et al. An Analysis of Network Literacy Education for Students in Private Universities in the Digital Age. *Media Forum*, 2025(04):108-111.
- [12] Li Y S. Practical Challenges and Collaborative Pathways of College Students' Network Literacy Education from the Perspective of Ideological and Political Education. *Henan Education (Higher Education)*, 2025(02):44-46.
- [13] Miao C X. Research on Improvement Strategies of Network Literacy Education for University Students in the New Era. *Heilongjiang Education (Theory & Practice)*, 2024(03):71-74.
- [14] Zhang M L. Research on the Content, Carriers, and Mechanisms of University Students' network literacy education in the Self-Media Era. *News World*, 2023 (06):112-115.