Article

Research on the Construction of Youth Network Literacy from the Perspective of Cyber Space Security

Yexin Zhang [1,*]

[1] Hainan Vocational University of Science and Technology, Haikou, Hainan, 571126, China
* Correspondence: Yexin Zhang, Hainan Vocational University of Science and Technology, Haikou, Hainan, 571126, China

Abstract: As the "fifth domain" of jurisdictional integrity, cyberspace has emerged as an indispensable frontier within the comprehensive framework for public safety and systemic social stability. Within this landscape, youth groups, as "digital natives" and the most active participants in the online ecosystem, possess a level of network literacy that is directly tied to the resilience of digital environment protection and the sustainable advancement of the strategic vision for a robust digital state. However, the rapid evolution of technologies—such as Generative AI, algorithmic recommendation engines, and deepfakes—has introduced unprecedented complexity into the online environment, creating new challenges for social order and individual development. This research, grounded in the strategic perspective of network safety, systematically evaluates the multidimensional impacts of the current network ecology on the cognitive frameworks, behavioral norms, and value systems of young individuals. The study identifies critical structural deficiencies in contemporary youth network literacy, particularly regarding proactive digital defense skills, information discernment in the face of "information cocoons," ethical-legal consciousness, and a profound understanding of the administrative integrity of the digital domain. To address these gaps, this paper proposes a "triad" educational framework that integrates Value Guidance, Capability Development, and Practical Empowerment. Furthermore, it advocates for a multi-stakeholder collaborative governance model involving regulatory bodies, educational institutions (with a focus on the practical strengths of vocational universities), social entities, families, and the youth themselves. This comprehensive approach aims to cultivate a new generation of "responsible netizens" capable of promoting public well-being while navigating the complexities of the digital age, thereby providing robust human capital for the construction of a safe and autonomous digital landscape.

Keywords: cyberspace security; youth groups; digital literacy; collaborative education; vocational education path

Published: 28 February 2026

1. Introduction

With the continuous and profound advancement of global digitalization and intelligent technologies, cyberspace has fundamentally evolved into a critical new dimension for social development and national governance, standing alongside the traditional physical domains of land, sea, air, and space [1]. In this era of ubiquitous connectivity, the security and stability of the digital environment have become increasingly intertwined with the broader framework of social harmony and sustainable development. According to the 55th *Statistical Report on China's Internet Development* released by the China Internet Network Information Center (CNNIC), as of January 2025, the number of internet users in China has reached 1.108 billion, with a penetration rate of 78.6%. Within this vast digital landscape, youth groups, primarily represented by university and vocational students, have emerged as the "resident citizens" and the most

active participants in various online applications. However, as the network ecosystem becomes more complex, emerging technical challenges such as sophisticated data privacy risks and the misuse of generative artificial intelligence, alongside social risks like online polarization and misinformation, have created a multifaceted environment that significantly impacts the development and security of the younger generation [2].

The period of youth is widely recognized in developmental psychology and sociology as a vital stage for the formation of stable worldviews, life perspectives, and core values. The behavioral patterns and value judgment capabilities exhibited by young people in cyberspace do not merely influence their individual growth and career prospects; they also serve as foundational elements that determine the overall resilience and civility of the collective network environment. Consequently, the concept of "Network Literacy" in the modern context has evolved into a comprehensive, multi-dimensional construct that extends far beyond rudimentary technical operations. A robust framework of network literacy now encompasses several critical pillars: first, the technical ability to recognize and mitigate cybersecurity risks; second, the cognitive capacity for critical thinking and information discernment in an era of algorithmic distribution; third, the ethical and legal awareness necessary to conduct oneself responsibly in virtual spaces; and finally, a profound understanding of the importance of maintaining a secure and orderly digital society. Cultivating these competencies is essential for ensuring that the youth can navigate the digital age with both confidence and a sense of social responsibility.

Despite their apparent proficiency in utilizing digital tools, a considerable gap remains between the current state of youth network behavior and the requirements of a high-quality digital society. Empirical research suggests that many young people still exhibit vulnerabilities such as inconsistent cybersecurity awareness, a tendency to rely on fragmented information, and a localized lack of clarity regarding the legal boundaries of online conduct. These issues are not aligned with the strategic goals for healthy youth development, which emphasize the importance of guiding the younger generation to use the internet in a scientific, legal, and rational manner. Therefore, conducting a systematic research into the construction of youth network literacy from the perspective of cyberspace security is of significant academic and practical importance. By exploring the mechanisms of how the online environment shapes youth behavior and identifying the structural shortcomings in their current literacy levels, this study seeks to propose a collaborative educational framework. Such an approach, involving multiple social stakeholders, aims to provide a solid foundation of talent and human capital for the long-term prosperity and security of the digital future.

2. The Multidimensional Impact of Cyberspace Security Environment on Youth

2.1. Young Individuals' Legitimate Rights Face Emerging Ccyber Threats

The rapid evolution of the digital landscape has exposed the youth to an increasingly sophisticated array of cyber threats that directly jeopardize their legitimate rights and personal safety. While this demographic is characterized by high technical engagement, their relatively limited social experience and underdeveloped risk-mitigation strategies make them prime targets for digital exploitation, including cyber fraud, systemic data breaches, and persistent online harassment. A critical issue is the "privacy paradox," where young users, in their pursuit of social validation and convenience, frequently neglect privacy protection by excessively sharing sensitive personal information across social platforms. This creates a permanent and vulnerable digital footprint that can be exploited by malicious actors. Furthermore, when their rights are infringed upon, a significant portion of the youth population lacks the requisite legal literacy and procedural knowledge to navigate complex defense channels. This inability to effectively utilize legal tools or technical skills for self-protection not only leads to immediate financial or psychological harm but also creates long-term vulnerabilities in their digital lives [3].

2.2. Cognitive Structures and Thinking Abilities Are Shaped Implicitly by Algorithmic Mechanisms

The cognitive development of the youth is increasingly influenced by the "black box" mechanisms of algorithmic recommendation systems, which prioritize engagement over information diversity. While these systems enhance information retrieval efficiency, they simultaneously construct pervasive "information cocoons" and "echo chambers" that restrict exposure to diverse viewpoints. Young people, immersed in homogeneous and fragmented content over extended periods, experience a gradual erosion of their capacity for sustained attention and deep, systematic thinking [4,5]. The "fast-food reading" culture, fostered by short-form videos and social media snippets, encourages superficial information processing rather than rational reasoning or critical inquiry. This cognitive narrowing hinders their ability to form comprehensive, objective, and multi-perspective views on complex social phenomena. Consequently, without a robust foundation of information discernment, the younger generation becomes increasingly susceptible to cognitive biases and the polarizing effects of curated digital realities.

2.3. Online Behavioral Misconduct Impedes Healthy Personal Development

The virtual and anonymous nature of cyberspace often weakens the moral constraints and social accountability that govern real-world interactions, leading to a visible rise in behavioral misconduct among youth. This "online disinhibition effect" can manifest as internet addiction, which encroaches upon essential time dedicated to formal education, physical exercise, and meaningful social interaction, thereby impacting both physical and mental well-being. In the realm of public discourse, a lack of rational judgment often leads young users to express emotions impulsively or engage in toxic behaviors such as cyberbullying and the dissemination of unverified rumors. Such actions not only infringe upon the rights and dignity of others but also obstruct the formation of a sound and resilient personality. The disconnect between virtual actions and real-world consequences makes it difficult for some youths to establish a mature sense of self-discipline, which is essential for navigating both digital and physical societies responsibly.

2.4. Cyberspace Serves as a Hub for Diverse Cultural Currents and Value-Based Challenges

As a primary arena for cultural exchange, cyberspace has also become a complex field where various subcultures and pervasive entertainment trends challenge mainstream values and traditional aspirations. The influence of social media influencers and commercialized trends often promotes negative cultural forces, such as extreme utilitarianism and materialism, leading some young people to adopt superficial value orientations. This shift can weaken their internal drive for self-improvement and academic excellence. The widespread adoption of nihilistic internet buzzwords, such as "lying flat" (tang ping) and "involution" (nei juan), serves as a digital reflection of their inner conflicts and confusion regarding their future roles in a competitive society. When young people utilize these terms for emotional release, it often indicates a deeper struggle with their value systems amidst a saturation of conflicting information. Without effective value guidance, this environment can lead to a fragmented sense of identity and a diminished commitment to social and civic responsibilities [6].

3. The Current Status and Structural Shortcomings of Youth's Internet Literacy

3.1. Proficient in Basic Operational Skills, but Weak in Cybersecurity Protection and Attention Management Capabilities

While contemporary youth are widely regarded as "digital natives" with high proficiency in navigating hardware and software interfaces, a significant gap exists between their operational fluency and their actual defensive capabilities. Most young people possess an intuitive grasp of social media, gaming, and productivity tools, yet their underlying cybersecurity awareness remains alarmingly superficial. There is a notable

lack of understanding regarding modern socio-technical threats, such as sophisticated phishing tactics, data encryption protocols, and advanced privacy settings. Furthermore, their grasp of the institutional frameworks governing digital safety-specifically the Cybersecurity Law and the Data Security Law-is often fragmented, leading to a failure to recognize how personal digital hygiene contributes to the broader stability of the national cyberspace ecosystem. Parallel to this technical vulnerability is the widespread crisis of digital attention management. Empirical research suggests that approximately 90% of college students spend upwards of three hours daily on digital devices, often falling victim to "dopamine loops" designed by attention-driven platforms [7]. This constant exposure to fragmented, high-stimulation content significantly impairs their capacity for deep concentration and sustained critical thinking, ultimately encroaching upon the time required for meaningful, real-world social engagement and academic reflection.

3.2. High Efficiency in Information Reception, but Lack of Information Discernment and Critical Thinking Skills

The internet has provided the younger generation with unprecedented access to a global repository of knowledge, yet this "information abundance" has not translated into high-level information literacy. Instead, many youths have developed a passive reliance on algorithmic recommendation engines, which prioritize engagement over accuracy or source diversity. This over-reliance fosters a "lazy" information-seeking habit, where users rarely venture beyond curated feeds, leading to the formation of "information cocoons" and "echo chambers." Within these digital silos, cognitive homogeneity flourishes, and the ability to discern truth from sophisticated misinformation becomes increasingly strained. Due to limited life experience and a lack of training in formal logic, many young people struggle to independently verify the veracity of online rumors or "fake news." Consequently, they often inadvertently become links in the misinformation chain by reacting to or sharing unverified content. At a deeper level, this reflects a structural decline in critical thinking; the inability to engage with diverse or dissenting perspectives leads to a superficial understanding of complex social issues, making the youth demographic particularly prone to group polarization and emotional volatility in digital spaces.

3.3. Strong Online Expression of Will, but Relatively Lagging Moral and Legal Awareness

Young people have emerged as the most dynamic and vocal force in the digital public square, yet the surge in their expressive activity has outpaced the development of their moral and legal consciousness. On the legal front, there remains a persistent misconception of cyberspace as a "lawless zone," where the boundaries of intellectual property, privacy rights, and defamation are poorly understood or ignored. Many youths unknowingly cross legal thresholds through unauthorized content sharing or data misuse, while simultaneously lacking the knowledge to seek legal redress when their own digital rights are violated. Morally, the "online disinhibition effect" caused by the perceived anonymity of the virtual world tends to dilute individual accountability. In many instances, this lack of social presence leads to a lowering of ethical standards, resulting in impulsive emotional outbursts, verbal abuse, or participation in cyberbullying [8]. This dilution of responsibility suggests that while young people are eager to assert their "digital presence," their sense of "digital citizenship"-which requires a balance between rights and responsibilities-remains underdeveloped. Without a clear understanding of the ethical boundaries of acceptable behavior, their strong expressive will can inadvertently contribute to a toxic and disordered online environment.

4. Path of Youth Network Literacy Construction from the Perspective of Cyberspace Security

To improve the youth's network literacy is a systematic project, which must adhere to the trinity concept of "value guidance, ability cultivation and practice empowerment",

and construct a multi-dimensional collaborative education mechanism among government, university, society, family and youth themselves.

4.1. Optimization of Higher Education System: Building an Integrated Education Model

As the primary arena for talent cultivation, universities should integrate digital literacy development throughout their educational processes. They must strengthen ideological and political guidance while embedding national security awareness. By incorporating cybersecurity concepts and national cyber sovereignty principles into ideological education courses, institutions can enhance young people's political acumen through case studies like the "PRISM scandal". Legal frameworks and ethical standards should form integral components of ideological education, guiding students to adopt law-abiding and responsible online behavior. To solidify theoretical foundations, universities should develop interdisciplinary general education modules covering network technology, information security, digital ethics, and legal systems. Cutting-edge topics such as AI security and data privacy protection should be promptly incorporated, with digital literacy education embedded in core courses like computer fundamentals and ideological and legal education. Practical training should be reinforced through cybersecurity labs and virtual simulation platforms, enabling students to master risk identification and emergency response skills through simulated exercises [9]. Encouraging student participation in cybersecurity outreach and community digital engagement initiatives helps bridge theory with practice. To cultivate interdisciplinary faculty, universities should recruit professionals with expertise in computer science, ideological education, and legal studies, establishing regular training mechanisms to enhance their ability to integrate cybersecurity knowledge with ideological education.

4.2. Building a Collaborative Governance System of Home-School-Community: Creating a Clean and Healthy Educational Environment

The government strengthens top-level design and optimizes cyberspace governance. It improves the legal framework for cybersecurity, intensifies law enforcement, and cracks down on cybercrimes. By leveraging technology, it enhances content oversight, reinforces platform accountability, refines algorithmic recommendation systems, and enhances "Youth Mode". Innovative approaches include using short videos and other youth-friendly formats for regular digital literacy education. Social forces actively participate in collaborative education. Internet companies should develop cybersecurity education products, provide practical opportunities, and enforce strict content moderation; mainstream media should guide public opinion, promote cyber civility, and highlight positive role models; social organizations can host digital literacy workshops and case studies to raise youth risk awareness. Families lay solid foundations through guidance and modeling. Parents should proactively improve their own digital literacy, learn cybersecurity knowledge, and set examples for their children's responsible internet use. By establishing family internet usage guidelines and discussing trending topics, parents can help children manage online time and resist temptations [10]. Strengthening school-community collaboration fosters joint educational efforts. Young people should develop self-driven growth by actively learning cybersecurity knowledge, improving information discernment and legal rights protection skills, establishing self-monitoring and evaluation mechanisms, regularly reflecting on online behavior to overcome addiction, and participating in building a civilized online environment by creating and sharing positive content while resisting vulgar and false information.

5. Conclusion

In conclusion, cybersecurity serves as the indispensable strategic cornerstone of national security in the digital age. Its comprehensive reinforcement relies not only on the advancement of technological "hard power" but, more crucially, on the cultivation of the

digital literacy of young people, who serve as the core actors and most influential nodes in contemporary cyberspace. While the younger generation currently possesses proficient basic online operational skills, this research highlights that they still exhibit notable structural gaps in critical cybersecurity awareness, sophisticated information analysis capabilities, ethical-legal consciousness, and a deep-seated understanding of national cyber sovereignty. These deficiencies represent the "human factor" in security risks that technology alone cannot fully resolve.

Looking ahead, as the technological horizon expands with the rapid advancement of generative artificial intelligence, big data analytics, and quantum computing, the complexity and deceptiveness of the cyber environment will only intensify. This necessitates an urgent and deepened approach to youth digital literacy development that evolves in tandem with these innovations. We must move toward a holistic educational model that balances value-based guidance with technical skill cultivation, ensuring that theoretical instruction is seamlessly integrated with practical empowerment through immersive exercises and real-world simulations. Furthermore, the optimization of university education systems must be complemented by a robust collaborative governance mechanism that effectively synergizes the efforts of families, educational institutions, social organizations, and the government.

By fostering a comprehensive environment that encourages individual self-discipline alongside institutional support, we can continuously enhance young people's cybersecurity awareness, legal and ethical standards, and sense of national identity. Only through this multi-dimensional approach can we nurture a new generation equipped with both robust digital competencies and a profound patriotic commitment. This strategic investment in human capital will provide a continuous and inexhaustible source of youthful energy, ensuring the steady, resilient, and secure progress of the nation as it navigates its path toward becoming a global cyber power.

Funding: 2024 Scientific Research Project of Hainan Vocational University of Science and Technology (No: HKKY2024-66) -Research on the Current Status and Improvement Strategies of Youth Digital Literacy in the New Era

References

1. Y. Dai, X. Tang, and C. Liu, "Research on the value and path of cultivating college students' digital literacy in the digital age," In *Proceedings of the 8th International Conference on Education and Training Technologies*, April, 2022, pp. 92-97. doi: 10.1145/3535756.3535771
2. S. Silvhiany, S. Huzaifah, and I. Ismet, "Critical digital literacy: EFL students' ability to evaluate online sources," *Indonesian Journal of EFL and Linguistics*, vol. 6, no. 1, p. 249, 2021. doi: 10.21462/ijefl.v6i1.364
3. E. Koza, "Information security awareness and training as a holistic key factor-how can a human firewall take on a complementary role in information security," *Human Factors in Cybersecurity. AHFE*, 2022.
4. H. Shrobe, D. L. Shrier, and A. Pentland, "New Solutions for Cybersecurity," *MIT Press*, 2018.
5. R. J. Green, "Attracting, Developing, and Retaining Cybersecurity Talent: Leadership Strategies for Bridging the Skills Gap (Doctoral dissertation, South College)," 2025.
6. C. Zhang, "Problems and Countermeasures in the Management of Computer Network Teaching in Colleges and Universities Based on the Era of New Media," In *The International Conference on Cyber Security Intelligence and Analytics*, March, 2021, pp. 66-73. doi: 10.1007/978-3-030-70042-3_10
7. F. Mokhtari, "Fostering digital literacy in higher education: Benefits, challenges and implications," *International Journal of Linguistics, Literature and Translation*, vol. 6, no. 10, pp. 160-167, 2023.
8. Y. K. Peker, L. Ray, S. Da Silva, N. Gibson, and C. Lamberson, "Raising cybersecurity awareness among college students," In *Journal of The Colloquium for Information Systems Security Education*, October, 2016, pp. 17-17.
9. H. Munasinghe, and K. Hewawasam, "Uniting Digital Disciplines: Bridging Literacy, Ethics, and Security Among University Students," In *2025 5th International Conference on Advanced Research in Computing (ICARC)*, February, 2025, pp. 1-6. doi: 10.1109/icarc64760.2025.10962887
10. J. Lourenço, J. C. Morais, S. Sá, N. Neves, F. Figueiredo, and M. C. Santos, "Cybersecurity concerns under COVID-19: representations on increasing digital literacy in higher education," In *Perspectives and Trends in Education and Technology: Selected Papers from ICITED 2022*, 2023, pp. 739-748. doi: 10.1007/978-981-19-6585-2_65