Dialectical Relationship and Collaborative Governance of Network Security from the Perspective of Information Literacy Path

Yang Zhang*

School of Public Education, Shandong University of Arts, Jinan, China

*1973107618@qq.com

Abstract. In the process of digital society transformation, network security has evolved from a purely technical issue to a systemic governance issue centered around people. The relationship between information literacy and network security presents a dialectical unity, with the two supporting, constraining, and transforming each other. This article takes dialectical materialism as the analytical framework to explain the inherent logic of information literacy and network security in terms of unity, opposition, and transformation. It points out the current practical difficulties in cognition, education, governance, and culture, and proposes a collaborative governance path from four dimensions: education system, technological empowerment, institutional guarantee, and cultural cultivation, providing theoretical support and practical reference for promoting the modernization of network security governance.

Keywords: information literacy, network security, dialectical relationship, digital governance, collaborative governance

1 Introduction

The deep integration of digital technology into social life has propelled human society into a new stage of intelligent civilization, while also presenting complex, covert, and large-scale risks in cyberspace. Traditional network security governance has long focused on technical protection, emphasizing hardware and software construction such as system reinforcement, firewalls, and intrusion detection, but generally neglecting the key variable of "people". A large number of cybersecurity incidents are caused by human negligence, inadequate cognition, and behavioral misconduct, indicating that the essence of cybersecurity has shifted towards "human centered security".

Information literacy, as the core competency of citizens in the digital age, is the key foundation for resisting network risks, regulating network behavior, and achieving secure autonomy. The relationship between information literacy and network security is not a simple linear relationship, but a dialectical relationship full of tension. The systematic interpretation of the internal logic, contradictory movement, and

C. F. Peng et al. (eds.), *Proceedings of the 2026 5th International Conference on Humanities, Wisdom Education and Service Management (HWESM 2026)*, Advances in Social Science, Education and Humanities Research 1024,
https://doi.org/10.2991/978-2-38476-593-5_29

transformation mechanism of the two is still relatively weak in current research. Based on this, this article starts from the perspective of information literacy, reveals its dialectical relationship with network security, analyzes practical difficulties, and constructs a collaborative governance path, providing new ideas for enhancing national network security capabilities.

2 Core Concepts and Dialectical Analysis Framework

2.1 The Connotation of Information Literacy in the Era

Information literacy is an essential ability for individuals in the intelligent era to survive and develop in cyberspace. Its connotation has expanded from traditional information retrieval to comprehensive literacy that integrates security, ethics, judgment, and skills. It mainly includes four dimensions:

Information risk awareness: able to identify potential threats such as fraud, rumors, phishing, malicious programs, etc.

Critical evaluation ability: the ability to distinguish and reflect on the authenticity, sources, and positions of information.

Information ethics and legal awareness: Respect privacy and property rights, abide by network rules and legal bottom lines.

Security practical skills: Master practical skills such as password management, privacy settings, emergency response, etc.

The data of public information literacy abilities are shown in Table 1[1].

Table 1. Proportion of Four Dimensions of Public Information Literacy Abilities

Dimension of Literacy	Proportion of people with basic abilities	Proportion of people with proficient abilities
Risk identification awareness	68.2%	21.5%
Critical evaluation ability	52.7%	13.8%
Ethical and Legal Awareness	71.3%	25.2%
Safety practical ability	45.9%	9.6%

Data source: 2024 National Citizen Information Literacy Sampling Survey

2.2 The Essential Characteristics of Network Security

In the digital society, network security is no longer limited to system and device security, but presents distinct characteristics of the times:

Systemic: Security threats spread across platforms, domains, and subjects;

Dynamics: Threat forms rapidly iterate with technology, and attack and defense continue to upgrade;

Sociality: Safety issues are highly linked to social governance and public interests;

Subjectivity: Human cognition, behavior, and literacy directly determine the level of safety.

These features collectively constitute the complex landscape of cybersecurity: systemic features highlight the "butterfly effect" of cyberspace, and vulnerabilities in a single intelligent device may trigger industrial control system paralysis through the IoT chain, such as cascading failures in energy pipelines and traffic signal systems; Dynamics manifest as an arms race in offensive and defensive technologies, with AI driven automated attack tools increasing zero day vulnerability exploitation efficiency by 300%, while defenders need to respond to unknown risks with continuously iterating threat intelligence; The sociality is reflected in the deep interweaving of data security and public interest. Medical data leakage endangers patient privacy, financial data tampering affects market stability, and network security has become the "infrastructure" for the development of the digital economy; Subjectivity reveals that the "last mile" of security protection lies with people. A survey of a data breach incident on an e-commerce platform showed that 78% of security vulnerabilities stem from employees' weak password habits, confirming the reality that "no matter how strict technical protection is, it is difficult to prevent people's cognitive blind spots". Relevant studies have systematically elaborated the essence of network security[4].

2.3 Dialectical Analysis Framework of Information Literacy and Network Security

This article is based on dialectical materialism and constructs an analytical framework from three levels: unity, opposition, and transformation, revealing the laws of their contradictory movements.

3 A Deep Analysis of the Dialetical Logic Between Information Literacy and Network Security

3.1 Unity: Literacy is the Foundation of Safety, and Safety is the Basis of Literacy

Information literacy is the first line of defense for network security and also the most sustainable 'soft defense'. Improving public information literacy can significantly reduce human risks and minimize the occurrence of security incidents.
The proportion of human-induced risks is shown in **Table 2.**

Table 2. Proportion of Human Induced Risks in Cybersecurity

Risk incentives	proportion
Weak password/password reuse	38.7%
Click on the phishing link	26.3%
Unauthorized disclosure of privacy information	19.5%
Security software not updated	10.1%
Other human negligence	5.4%

Data source: National Network and Information Security Information Notification Center (2024)

More than 80% of cybersecurity incidents are caused by human factors, fully demonstrating that information literacy is the core support of cybersecurity [3]. At the same time, the improvement of the network security environment also provides a healthy space for the enhancement of information literacy, and the two complement each other.

3.2 Oppositionality: The Dynamic Tension between Freedom and Order

There is an inherent contradiction between information literacy and network security in their development: 1 There is a tension between information freedom and security control; 2. Technological dependence may lead to the degradation of individual safety capabilities; 3. The digital divide makes vulnerable groups high-risk groups.

Freedom of information is the foundation of digital civilization, but absolute freedom may lead to risks such as rumors and fraud. Security control can maintain network order, but excessive control can inhibit information flow, reflecting the game between individual rights and public interests. Technological dependence leads to the degradation of security capabilities, intelligent tools reduce users' awareness and skills of protection, and AI systems may solidify cognition and weaken critical abilities. The digital divide transforms differences in information literacy into security inequalities, with vulnerable groups at higher risk. Ignoring differences in security measures may exacerbate distribution imbalances.

The literacy level and risk rate of different groups are shown in Table 3[2]. The elderly and rural residents exhibit characteristics of low literacy and high risk,and the digital divide exacerbates the security imbalance[5].

Table 3. Information Literacy Level and Risk Exposure Rate of Different Groups

group	Comprehensive score of literacy (100 points)	Network risk encounter rate
Teenagers (12-18 years old)	62.3	32.6%
Middle aged and young adults (19-59 years old)	78.5	15.8%
Elderly people (over 60 years old)	41.7	47.2%
rural residents	53.6	39.4%
urban residents	72.1	18.3%

Data source: CNNIC's 53rd Statistical Report on Internet Development in China (2024)

The elderly and rural residents exhibit characteristics of low literacy and high risk, and the digital divide exacerbates the security imbalance.

3.3 Transformability: The Spiral Rise from Technology Dominance to Literacy Empowerment

The transformation path of information literacy and network security follows the law of "negation of negation" and achieves dynamic upgrading. The transformation path is as follows:

Technology defense as the main focus → Threat complexity, technological effectiveness decline → Shift towards information literacy cultivation → Individual proactive immunity,

Overall security improvement → Flexible governance, healthier information flow → Further upgrading of literacy, continuous strengthening of security →

Technical defense as the main focus (cyclic rise)

This path reveals that network security governance ultimately moves towards the synergy of technology and literacy.

4 Reality Dilemma

4.1 Cognitive Dilemma: Deep-rooted Technology Centrism

Heavy emphasis on technology over personnel, heavy emphasis on equipment over awareness, resulting in low efficiency in safety investment. Some organizations still adhere to the investment model of "emphasizing hardware over software" in network security construction, with hardware procurement and software upgrade budgets accounting for over 70%, while "software investment" such as personnel literacy cultivation and behavior norms construction accounts for less than 15%. This imbalance in resource allocation has led to a "strong on the outside and weak on the inside" feature of the security system: technical defenses such as firewalls and intrusion detection systems are becoming increasingly sophisticated, but the proportion of "insider threats" caused by weak risk awareness among internal personnel is increasing year by year, reaching 42% of the total number of security incidents by 2024. What is even more alarming is that technology centrism has given rise to a "tool dependency syndrome", where some managers equate security measures with simply stacking technology products, ignoring the standardized guidance of employees' daily operational behavior, and forming a cognitive misconception that "purchasing more advanced security equipment can solve problems". When faced with new social engineering attacks, even with advanced threat detection systems deployed, personnel often fall into a passive cycle of "technology upgrade threat mutation re upgrade" due to a lack of discernment ability, which seriously restricts the sustainable improvement of network security governance effectiveness.

4.2 Education Dilemma: Fragmentation and Formalization of Information Literacy Education

Lack of systematic courses, insufficient coverage of key groups, and a lack of practical training. Currently, information literacy education in primary and secondary schools is mostly scattered in scattered chapters of information technology courses, lacking integration with subjects such as Chinese language and ideological and political education, and presenting a "silo like" feature in the knowledge system; Although information security related courses are offered in higher education, they are mostly aimed at computer science students, and the coverage rate of general education is less than 30%; Vocational training focuses more on skill operation and lacks the cultiva-

tion of advanced abilities such as ethical judgment and risk assessment, resulting in an educational gap of "elementary school shallow taste, university professional differentiation, and adult training gap". There is a significant imbalance in the coverage of key groups, and digital education for the elderly mainly focuses on the use of basic equipment, with insufficient involvement in security content such as fraud identification and privacy protection. According to a special survey in 2024, only 12.7% of elderly universities offer cybersecurity courses; Rural areas are limited by teachers and equipment, and the implementation rate of information literacy education is less than one-third of that in urban areas. Left behind children lack family guidance, and their risk identification ability is 28.5 percentage points lower than their urban peers. Practical training is generally lacking, and existing education mostly adopts a static mode of "PPT lectures+case analysis", lacking immersive training such as simulated phishing email recognition, malicious link detection, emergency response, etc., resulting in learners "understanding theory but not operating". An experiment at a certain university shows that students who receive traditional teaching have a recognition accuracy rate of only 43% in simulated fraud scenarios, while the accuracy rate of the group who have undergone practical training can reach 89%. The disconnect between theory and practice directly weakens the actual effectiveness of education.

4.3 Governance Dilemma: Lack of Collaborative Mechanisms Among Multiple Stakeholders

The performance of governance subjects is shown in **Table 4**.

Table 4. Performance Status of Network Security Governance Entities

Governance subject	Performance rate	main issue
government	65.4%	Fragmented planning and insufficient collaboration
enterprise	42.8%	Prioritizing profit over safety responsibility
school	37.2%	Formal education, lacking practical experience
family	29.6%	General lack of safety guidance
social organization	31.5%	Low participation and narrow coverage

Data source: Cyberspace Governance Survey by the Cyberspace Administration of China (2024)

4.4 Cultural Dilemma: A healthy Online Ecosystem has Not Yet Formed

The ethical foundation is weakened by issues such as rumors, privacy breaches, and traffic fraud in cyberspace, resulting in the phenomenon of "bad money driving out good money": short video rumors spread through algorithm fission, and the reach rate of debunking is low; The misuse of personal information has led to a crisis of trust among the majority of netizens towards the platform; Traffic fraud distorts content orientation, drowning out high-quality content and creating a vicious cycle of vulgar profit. This leads to the collapse of the online integrity contract, rational discussion

giving way to emotional venting, individual judgment being lost, and the difficulty in forming a consensus on social network security ethics.

5 Collaborative Governance Path

5.1 Building a full Cycle, Hierarchical and classified Information Literacy Education System

Incorporate information security literacy into national education and conduct specialized training for young people, the elderly, and rural residents. Integrating compulsory education curriculum into the basic education stage, developing a spiral progression curriculum from primary school to junior high school: cultivating risk perception in primary school, introducing interactive practice in junior high school, and deepening critical thinking in high school. Building a dual track system of "general education+majors" in higher education, offering compulsory courses to all students, advanced courses for different majors, and establishing school enterprise practice bases to enhance practical skills. Professional groups are implementing industry-specific customized training, while industries such as finance and healthcare are strengthening their professional content. Civil servants emphasize confidentiality education, while small and medium-sized enterprises focus on basic protection and establish industry certification and assessment standards. Targeting the elderly and rural population, breaking through the digital divide, and offering key lectures on anti fraud knowledge such as the "Silver Age Classroom".

5.2 Promote Dual Wheel Drive of Technological Empowerment and Humanistic Protection

Enhance early warning capabilities with intelligent technology and strengthen humanistic defense with literacy education. In terms of technology, we will build an intelligent threat perception system, use AI to monitor network behavior in real time, integrate information to establish threat profiles, and achieve proactive warning. Develop anomaly detection models, establish behavioral baselines, and achieve risk second level warnings. Using natural language processing to analyze public information and identify risks, combined with knowledge graphs to trace the source. In the field of privacy protection, promote technologies such as federated learning and differential privacy to ensure data security and compliant circulation.

In terms of humanities, we will strengthen the concept of "people are the first line of defense" and cultivate individual defense abilities through scenario based education. Develop an immersive training system to simulate risks and enhance emergency response capabilities. Establish ethical constraint mechanisms and incorporate information ethics into norms. Build a nationwide reporting platform to encourage supervision, form a closed-loop protection network of "technical warning humanistic response social supervision", and achieve a dynamic balance between technology and humanities.

5.3 Improve the Institutional Guarantee System with Clear Rights and Responsibilities

Consolidate platform responsibilities, improve safety and credit mechanisms, and strengthen interdepartmental collaboration. The platform should establish a 'safety first responsibility system', incorporate safety into product development and evaluation, and establish a rapid response mechanism. At the same time, cultivate user safety literacy and incorporate safety behaviors into credit evaluations. The safety credit mechanism needs to establish a "evaluation reward punishment repair" closed loop, classify and manage enterprises, and take corresponding reward and punishment measures. Personal credit can be linked to public services. Multi departmental collaboration should establish a collaborative governance network, horizontally form coordination groups to share intelligence, vertically establish three-level linkage to achieve rapid disposal, and improve cross regional law enforcement cooperation to form a global synergy.

5.4 Cultivate a Culture of Integrity, Rationality, and Responsibility in Cybersecurity

Promote the formation of a common value of "understanding safety, guarding safety, and protecting safety" in the whole society. A culture of integrity requires the establishment of a "behavior evaluation feedback" loop and online integrity archives, with evaluation content and cross platform rewards and punishments. Platforms should optimize algorithms to build an "integrity is value" ecosystem. Strengthening rational thinking requires enhancing information processing abilities, setting up screening courses in basic education, ensuring the credibility of information on media platforms, and guiding rational discussions through factual verification by professional institutions. To implement the sense of responsibility, it is necessary to establish a three-level system of individuals, organizations, and society, combining safety commitments, behavioral assessments, and cultural activities to make maintaining safety conscious. Build a multi-party collaborative cultural cultivation ecological chain, where the government, enterprises, social organizations, and families each play their respective roles, forming a closed loop of guidance, infiltration, and practice, and transforming safety concepts into national actions.

6 Conclusion

Information literacy and network security are an organic whole of the digital social security system, presenting a dialectical relationship of unity, opposition, and transformation. Information literacy is the human foundation of network security, and network security is the environmental guarantee of information literacy. In the face of new risks in the era of intelligence, it is necessary to abandon technology centrism and shift towards a new model that emphasizes human technology collaboration, education, and governance. By building a full cycle literacy education system, strengthening technological empowerment, improving institutional guarantees, and cultivating

a security culture, it is possible to achieve a positive interaction, dynamic balance, and collaborative improvement between information literacy and network security, providing solid support for building a strong cyber nation[6].

References

1. UNESCO Global Information Literacy Report [R]. Paris: UNESCO, 2023
2. China Internet Network Information Center The 53rd Statistical Report on Internet Development in China [R]. Beijing: CNNIC, 2024.
3. Shen Zhiyuan Research on the Interactive Relationship between Citizen Information Literacy and Network Security in the Digital Age [J]. Intelligence Theory and Practice, 2023
4. Fang Binxing The essence and future development direction of network security [J]. Journal of the Chinese Academy of Sciences, 2022
5. Van Dijk J A G M. The Deepening Divide: Inequality in the Information Society[M]. London: Sage Publications, 2022.
6. Wilson P. Information Literacy as a Core Component of National Cybersecurity Strategy[J]. Journal of Information Ethics, 2022.