Holistic Intelligent Governance of Online Information Content Ecosystem Security Risks: Theoretical Framework and Implementation Strategies (Postprint)

Authors: Zhou Yi, Zhang Xue

Date: 2023-04-01T15:51:24+00:00

Abstract

[Purpose/Significance] Network information content ecological security risk constitutes a novel category of information ecological security issues that impact and threaten overall national security across multiple dimensions. [Method/Process] Grounded in holistic governance and smart governance theories and informed by technology mediation theory, this study proposes the conceptual framework, logical relationships, and fundamental content for constructing a theoretical framework of holistic smart governance for network information content ecological security risks, and elaborates specifically on the significance of this framework construction. [Results/Conclusions] Research indicates that the theoretical framework for holistic smart governance of network information content ecological security risks represents an organic integration of holistic and smart governance mediated by information technology. To advance its concrete organizational implementation, implementation pathways may be selected from dimensions including the construction of an institutionalized mechanism guarantee system and the implementation of an intelligent technology support system.

Full Text

Research on the Theoretical Framework and Implementation Strategy of Holistic Intelligent Governance for Ecological Security Risks of Network Information Content

Zhou Yi, Zhang Xue

School of Sociology, Soochow University, Suzhou 215123
Center for Data Governance and Industrial Development, Soochow University, Suzhou 215123

Abstract:
[Purpose/Significance] The ecological security risk of network information content represents a novel category of information ecological security issues that affect and threaten overall national security across multiple dimensions. [Method/Process] Grounded in theories of holistic governance and intelligent governance, and drawing on technological mediation theory, this paper proposes the conceptual foundations, logical relationships, and core components for constructing a theoretical framework for holistic intelligent governance of network information content ecological security risks, and specifically elaborates on the significance of this framework construction. [Result/Conclusion] The research demonstrates that the theoretical framework for holistic intelligent governance of network information content ecological security risks constitutes an organic fusion of holistic and intelligent governance mediated by information technology. To advance its concrete implementation, implementation pathways can be selected through establishing an institutionalized mechanism guarantee system and implementing an intelligent technical support system.

Keywords: ecological security risk of network information content; holistic intelligent governance; theoretical framework; implementation path

1 Research Progress and Problem Statement

1.1 Research Progress Analysis

Current scholarly research on network information content security risks both domestically and internationally primarily encompasses the connotation and manifestations of network content security risks, as well as interpretations of governance connotations and models. Early conceptions of network information content security mainly focused on content leakage, cyber espionage, and network spam resulting from system vulnerabilities, emphasizing security attributes such as confidentiality, integrity, and availability of information content. Contemporary understanding primarily concerns data content leakage itself and the production or dissemination of non-compliant or harmful network information. Across different periods, the manifestations of network information content security risks have varied in emphasis: (1) Traditional risks primarily involved the security of information systems, network structures, and network content per se. (2) Current risks are gradually evolving toward a complex of content security risks represented by privacy risks, national discourse power and ideological security risks, content vulgarization risks, content manipulation risks, intellectual property risks, and memory disappearance risks. These different risk types generate distinct impacts: privacy and intellectual property risks primarily threaten public interests and citizens' legitimate rights; information content manipulation risks endanger national and social security; discourse power and ideological risks undermine national credibility and political security; content vulgarization risks affect socialist core values and cyber civilization construction; and network memory disappearance risks threaten national memory and cultural heritage security.

The academic and professional communities have profoundly recognized the potential impacts and latent dangers of these various network information content security risks, and have conducted preliminary research on governance elements and models. Scholars acknowledge that the essence of network information content security risk governance lies in preventing content abuse and controlling the flow of harmful information, involving measures such as content classification, filtering, deletion, monitoring and early warning, and privacy protection. Some researchers argue that governance subjects primarily comprise government, enterprises, social organizations, and citizens, each holding different positions and playing distinct roles in network content security and cyberspace governance, employing legal policies, self-discipline conventions, and technical tools in governance practices that can form certain interactive relationships and produce governance effects. Research on governance objects has focused on user-generated content quality, emergency events and network public opinion security, cyberspace security, network infringement and information security, data openness security, and governance of negative network information. Regarding governance tools or models, scholars have analyzed from perspectives of policies and regulations, industry norms and information ethics, and technical means and tools, initially forming three typical models: government regulation, multi-stakeholder governance, and network autonomy.

In summary, existing research in this field has preliminarily revealed the elements, causes, and typologies of network information content security risks, but these explanations remain relatively fragmented. Research generally focuses on supervising negative information content as the primary governance object to form governance methods, without explicitly defining the connotation of network information content ecological security, and without conducting fine-grained analysis, evolution trend characterization, or holistic governance practices of network information content ecological security risks. Although recognizing that network information content ecological security risk governance involves multi-stakeholder actions and theoretically proposing several governance models, actual operations still primarily adopt dispersed, temporary, and extensive campaign-style governance targeting specific thematic content or network information service platforms, with governance actions characterized by obvious temporariness and dispersion, leaving considerable room for improvement in intelligent and precise governance.

1.2 Problem Statement

Under Web 2.0, User-Generated Content (UGC) has become the norm for network information content production. The diversity of user behaviors and the complexity of motivations for content generation have increased network information content ecological security risks. The flow and dissemination of various non-compliant or harmful information content exert significant impacts on overall national security from political, cultural, and economic dimensions. In response to the requirements of overall national security and the modernization

of the network governance system and governance capabilities, and considering the characteristics of UGC content organization and dissemination and policy developments such as the "Regulations on the Governance of Network Information Content Ecology" and the "Internet Information Service Management Measures" (revised draft), the transformation from supervising network harmful information content to governing network information content ecological security risks has become an important theoretical and practical issue, making research on governance model transformation or construction essential.

2 Theoretical Framework for Holistic Intelligent Governance of Network Information Content Ecological Security Risks

2.1 Network Information Content Ecological Security Risk Governance and Its Components

Network information content ecological security risk governance refers to the process whereby government-led multiple stakeholders, by employing big data technology, artificial intelligence technology, and other tools, target network information content ecological security risks as the governance object. According to certain rule systems, they promote effective coordination among multiple stakeholders to achieve precise, efficient, and orderly governance of network information content ecological security risks, thereby constructing a favorable network information content ecological security environment. The governance components included in this concept mainly comprise:

2.1.1 Governance Subject Elements

Network information content ecological security risk governance includes various stakeholders—all participants in the governance action field of network information content ecological security risks—primarily consisting of party committees and governments at all levels and their cyberspace administration departments as managers, internet industry organizations, network information service platforms (such as ICPs as content producers and ISPs as dissemination service providers) that serve as both governance subjects and governance counterparts, and users who act as content producers, disseminators, and consumers. Among these subjects, network information service platforms function as both governance subjects and governance counterparts, with their roles shifting across different governance scenarios.

2.1.2 Governance Object Elements

Network information content ecological security risk governance targets network information content ecological security as its object. Theoretically, network information content governance has two different orientations: the supervision of harmful information content and information content ecological security. Governance oriented toward harmful information content emphasizes state control over network information content quality, whereas governance oriented toward information content ecological security treats both positive and negative infor-

mation content as governance objects, maintaining a favorable overall content aggregation pattern through counter-indicative governance. Logically, network information content ecological security risk governance centers on "content aggregation patterns," involving not only supervision of harmful information content but also active production and distribution of positive information content—a form of counter-indicative governance between positive and negative information content. It concerns not only the "quantity" or "quality" of information content but also the diverse aggregation patterns of network information content. Therefore, from the perspective of governance object orientation, actual governance objects should more prominently emphasize the holistic and systematic governance of network information content ecological security risks.

2.1.3 Governance Tools and Technology Elements

Tools and technology elements include both administrative management means and related tools, as well as technical means and tools. From a developmental perspective, technical tool elements are gradually becoming the key core component of network information content ecological security risk governance. Big data technology, information identification and filtering technology, information integration processing technology, and intelligent service technology are all core guarantees for network information content ecological security risk governance.

2.1.4 Governance Rules and Institutions

Rules and institutions include cybersecurity laws and regulations, cyberspace and community management organizational structures, network information service platform content management processes, and network information service industry norms. These rule systems can be roughly divided into institutional rules and technical rules. Institutional rules mainly include laws and regulations (such as the Cybersecurity Law and Internet Information Service Management Measures) and related network policies (such as virtual community policies, network market policies, and network dispute mediation policies). Technical rules can be understood from two levels: from the perspective of implementing governance technical operation processes, holistic governance requires establishing a "multi-party linkage, three-dimensional co-responsibility" rule system; from the perspective of information technology application requirements for implementing governance, standards and protocols should be established for technical sharing and technical security among relevant subjects.

2.1.5 Governance Process Mechanisms

Governance involves constructing a network information content ecological security risk governance system based on deconstructing content ecological security risk scenario elements. Content ecological security risk scenario element deconstruction entails conducting holistic characterization of the current status and evolution trends of network information content ecological security risks from perspectives such as risk types, content clustering, value orientation, and dissemination nodes, to understand the relationships between risk types and risk responsibility sources and consequences, as well as between risk types and risk identification methods and governance departments. Content ecological secu-

rity risk governance system construction aims to build a multi-party linkage, intelligent-driven, three-dimensional co-responsibility network information content governance mechanism. Multi-party linkage refers to effectively integrating all forces including party committees, governments, enterprises, and social forces to form a multi-stakeholder collaborative governance mechanism led by party committees, managed by governments, with enterprises fulfilling responsibilities, supervised by society, and with netizen self-discipline. Intelligent-driven means that on the basis of leveraging manual review mechanisms, it is essential to fully utilize big data technology, artificial intelligence technology, etc., to flexibly customize different content security risk review strategies according to network information content product forms. Three-dimensional co-responsibility refers to clarifying authority and responsibility boundaries, standardizing the functional relationships among subjects through boundary demarcation, establishing power and responsibility systems for different subjects, thereby enhancing governance capabilities for network information content ecological security risks.

The network information content ecological security risk governance model constituted by the above elements will form different governance models due to differences in combination structures, operational organization mechanisms, institutional rule systems, and governance emphases. As previously identified, three typical models have currently emerged in domestic and international cyberspace governance and network information content security governance: government regulation, multi-stakeholder governance, and network autonomy. While these three models have achieved notable results in China's network information content ecological security risk governance practices, current research still focuses on specific topics or network information service platforms, adopting dispersed, temporary, and extensive campaign-style governance. How to construct a highly organized, ecologically holistic, normalized, and refined content ecological security governance system from a theoretical framework perspective based on the above governance components has become key to improving the modernization of the network governance system and governance capabilities.

2.2 Theoretical Framework for Holistic Intelligent Governance of Network Information Content Ecological Security Risks

In the 1990s, British scholar Andrew Dunsire proposed the concept of "holistic governance," which Perry Hicks later developed into "holistic governance theory." The core connotation of holistic governance lies in coordination and integration, requiring consensus and mutual cooperation between government departments and market sectors, social organizations, or private entities—it represents a new governance model featuring multi-stakeholder, collaborative, and coupled governance. Intelligent governance is a novel governance model proposed within the wave of "technocracy." The logic of intelligent governance belongs to the logic of technical governance, forming a three-dimensional foundation of technology-driven, institution-confirmed, and concept-supported governance. From these theoretical formulations, holistic governance and intelligent

governance share close internal connections and can achieve organic integration rather than simple addition. Based on holistic governance and intelligent governance theories, using technological mediation theory as the connection, and employing information technology to eliminate and break through the boundaries of fragmented subjects, this paper constructs a theoretical framework for holistic intelligent governance of network information content ecological security risks. This framework refers to achieving holistic, systematic, precise, and intelligent governance through extensive application of digital technology and artificial intelligence technology to promote effective coordination among governance subjects.

As shown in Figure 1 [Figure 1: see original paper]:

Figure 1. Theoretical Framework for Holistic Intelligent Governance of Network Information Content Ecological Security Risks

In constructing this holistic intelligent governance theoretical framework, the primary construction logic and approach are:

2.2.1 Governance Logic for Integrating Holistic and Intelligent Governance

In constructing the theoretical framework for holistic intelligent governance of network information content ecological security risks, particular attention should be paid to the combination of governance subjects, objects, tools, processes, and rules from both holistic and intelligent governance perspectives, thereby forming a fused governance logic of holism and intelligence. This fused governance logic employs information technology as an intermediary to promote coordinated linkage among multiple stakeholders, facilitate counter-indicative governance of positive and negative information, ensure smooth operation of content ecological security risk governance mechanisms, and ultimately achieve the governance goals of a clean network ecology and clear cyberspace. Analysis of this fused governance logic can be conducted from the integration process of governance subjects, objects, mechanisms, and results.

(1) **Governance Subject Perspective.** Holistic intelligent governance primarily addresses issues such as unclear governance subject boundaries, ambiguous authority and responsibilities, and weak coordination. The main concept and approach of the theoretical framework construction involve clarifying authority and responsibility subjects, demarcating governance boundaries, and forming governance synergy. The concrete effectiveness manifests as refined authority and responsibility lists for various subjects and the formation of a relatively complete system of subject division of labor, cooperation, and coordination mechanisms. Currently, as relevant government departments transfer their network content supervision powers to network information service platforms, these platforms become both governance subjects and governance counterparts, causing their actions to inevitably oscillate between normative responsibilities and actual practices, while the profit-driven nature of platforms further amplifies content

ecological security supervision risks. Therefore, how to authorize network information service platforms represents a form of governing the governors, and implementing detailed power lists and responsibility lists should be key to constructing coordination mechanisms among different governance subjects.

(2) **Governance Object Perspective.** Holistic intelligent governance primarily addresses problems such as the proliferation of harmful or non-compliant information content and insufficient production and distribution of positive energy content. The main concept and approach involve employing multiple means to obtain and process object information content, including manual and intelligent identification, filtering, and removal of non-compliant or harmful information content, as well as active production and distribution of positive energy content. This promotes a shift in governance object orientation from "harmful content" supervision to the overall pattern of "content ecology," and from governance of individual or partial network information content service platforms to holistic governance of cyberspace ecological security. The holism of governance objects emphasizes panoramic observation of network information content ecological security risks, treating risk manifestations and their interrelationships as a system rather than simply targeting specific content security risks, information service platforms, or content security topics. The transformation should be from "case-based" selective governance to holistic governance of "content aggregation patterns."

(3) **Governance Mechanism Perspective.** The primary distinction between holistic intelligent governance and existing governance models lies in abandoning single governance processes and singular governance object orientations to address issues such as temporariness and fragmentation in governance initiation processes and reliance on manual content review and post-hoc deletion. The main concept and approach of holistic intelligent governance framework construction involve designing intelligent, panoramic, normalized, and full-process content ecological security governance mechanisms. This is not limited to risk response but should also include establishing risk contexts, identifying risk natures, and assessing risk elements to gain initiative and control in the face of risks—a dynamic governance process. Ideally, governance subjects should be able to consider how to absorb disturbances caused by risk factors to the network content ecology based on the logic of content ecological security risk generation and restore it to its original state, while also using this as an opportunity for reflection to explore the fundamental causes behind network content ecological security incidents and crises.

(4) **Governance Result Perspective.** Holistic intelligent governance primarily addresses issues such as the contingency of governance results, the possibility of security risks occurring, and potential changes in user experience due to governance. Given that network harmful or non-compliant

information content features multiple coverage scenarios, numerous data variants, strong adversarial characteristics, and high concealment, the main approach of holistic intelligent governance framework construction should focus on how to use technical means to break through the "boundary" limitations imposed by society on subjects in content ecological security governance across departments, regions, and industries, and to overcome the individual governance limitations of different network information service platforms. The openness and inclusiveness pursued by holistic intelligent governance can situate specific content ecological security risk issues within the overlapping intersections of network communities and social relationships, emphasizing overall governance effectiveness rather than the resolution results of single content security risk issues or events. The concrete effectiveness manifests as precise identification of network content ecological security risks, clear overall governance processes, smooth content flow, and good user experience.

2.2.2 Leveraging the Intermediary and Connecting Role of Information Technology

Phenomenological technology studies indicate that technology often "assists" in shaping the context for its functional realization, shapes people's actions and perceptions, and constructs new practices and lifestyles. Phenomenology terms this phenomenon "technological mediation." In network information content ecological security risk governance, highly developed information technology can promptly respond to complex and voluminous information, facilitate information interaction among governance subjects, and thereby help establish correlations among relational subjects. It can assist and achieve linkage among different governance subjects (integration of vertical hierarchical relationships, coordination of horizontal subject relationships), associative identification of different content ecological security risk elements, and coordination of different governance processes, forming a "networked," "multi-centered," and "integrated" governance pattern that achieves dynamic balance among cyberspace public interests, network information service platform interests, and user personal experiences, thereby demonstrating tolerance and integration of heterogeneous network content spaces.

In constructing the holistic intelligent governance theoretical framework, the intermediary and connecting role of modern information technology also has its internal technical logic and specific scenarios: (1) Modern information technology can create new ways to identify and analyze content ecological security risks and their overall security states. Through real-time sensitive vocabulary identification, it enables fine-grained analysis of content ecological security risks, using data and its correlations to portray the real scenarios and evolution trends of network information content ecological security risks, thereby achieving high-precision governance of different types or dimensions of network information content ecological security risks. (2) Modern information technology can create new forms of automated network information content review and filtering. For

example, various intelligent content review systems have been promoted and applied in recent years, with core components including sensitive word detection, manual intervention operations, sensitive information replacement, and score feedback subsystems. These systems use search technology to identify sensitive words in content, automatically replace them, and include manual intervention components (modifying misjudgments and missed judgments) to ensure the effectiveness and accuracy of network information content identification. This not only greatly improves content review efficiency but also enhances the reliability and precision of content security risk review through human-assisted judgment. (3) Modern information technology can create automated production methods for network information content products. Research indicates that through in-depth analysis, mining, and utilization of massive data, automated news content production by machines around specific themes has become possible. For example, Tencent's DreamWriter can automatically generate manuscripts based on algorithms in the first instance, instantly output analysis and judgments, and deliver important information and interpretations to users within one minute. This automated content production form can greatly enhance the production and distribution intensity of positive energy information content products in cyberspace. (4) Modern information technology can create new methods for assessing the governance status of network content ecological security risks. For example, various network information service platforms can use the massive data and computational advantages of big data platforms to create precise user profiles, analyze and characterize different users' content generation interests and features, promptly identify sources of harmful or non-compliant information content and their risks, and thereby better conduct technical "verification" of trends in user-generated content and governance needs, determining priorities in content ecological security risk governance and rationally allocating internal platform resources.

2.2.3 Pursuing Dual Goals of Governance Efficiency and Value

Holistic intelligent governance emphasizes the efficiency of content ecological security risk governance, considering both the rationality and legality of governance actions and the efficiency and coordination of governance processes. The theoretical framework of holistic intelligent governance aims to use modern information technology to resolve conflicts and disorder caused by value differences, interest differences, and rule differences among departments, levels, platforms, functions, and groups in network information content production, distribution, and dissemination. Through the integration of technocracy, rule of law, and ethical governance, it integrates the decentralized governance objectives presented in the heterogeneous spaces of network information service platforms into network information content ecological security governance objectives, strategically responding to the needs of overall national security. From the perspective of theoretical framework construction, due to the intermediary and connecting functions of information technology, all participating subjects can adopt the posture of "one collaborative subject" or the logic of collective action to conduct all-round, all-weather identification and analysis of content

security risks, which can partially replace capability requirements for single governance subjects. In the research and development of relevant governance tools or solutions, the organization of technical forces from network information service platforms by relevant government departments to jointly develop content feature information databases and develop universal content review or filtering systems has become key to realizing technical review. Existing practices indicate that these ideas can be realized to varying degrees, thereby enhancing the effectiveness of network information content ecological security risk governance.

The public value pursued by the holistic intelligent governance theoretical framework manifests at two different levels: overall national security and network user participation experience. (1) Macroscopically, the public value objective pursued by holistic intelligent governance of content ecological security risks involves starting from the various manifestations of content ecological security risks, and through specific network content governance processes such as identification, retrieval, filtering, deletion, production, and distribution, constructing a dynamic security collection integrating political security, cultural security, and information security, thereby comprehensively achieving the public value objective of overall national security. (2) Microscopically, users' network participation behaviors have specific motivations or objectives, such as entertainment, political participation, publicity and display, commentary and suggestions, and economic interests. After years of internet practice and debate, consensus has been reached in both political and academic circles on internet governance: following the rule of law principle and implementing limited freedom. Users have the right to use network public spaces for expression but must participate in network activities within legal boundaries. The public value pursued by holistic intelligent governance microscopically manifests as seeking to balance the maximum common divisor of interests among network information service platforms and user subjects, enabling platforms to achieve profit objectives while users obtain good communication experiences.

The construction logic and approach of the holistic intelligent governance theoretical framework can fully demonstrate the rationality and effectiveness of network information content ecological security risk governance: (1) Holistic intelligent governance emphasizes multi-subject, multi-dimensional, multi-element, and multi-mechanism governance of network information content ecological security risks. This holistic theoretical framework construction does not simply equate a network service platform, network community, or certain thematic or event domains' content security hazards with network information content ecological security risks. "Content security risks" may evolve into crises or hazard events of harmful or non-compliant information content dissemination, but may also, through identification and early warning of risk sources, prompt various participating subjects to disperse, transfer, and eliminate content ecological security risks through multiple positive information distribution mechanisms and active counter-indicative governance and value guidance. The holistic intelligent governance theoretical framework construction can provide systematic concepts and methodological guidance for the holistic transformation of "content aggrega-

tion patterns" and maintenance of favorable ecological states. (2) Holistic intelligent governance emphasizes full-process and intelligent governance of content ecological security risks. Full-process and intelligent governance requires governance work to address all aspects including content security risk monitoring and prevention, analysis and assessment, risk dispersion and elimination, and response and disposal after harmful content security incidents. From the perspective of information lifecycle theory and network information content dissemination evolution laws, network information content generation, dissemination, variation, transformation, and disappearance also follow a dynamic evolution process. Previous attention to network information content security risk issues generally focused on response and disposal after security risk problems were clearly exposed or security risk events occurred, as evidenced by annual "thematic" or "special" campaign-style network governance. The full-process and intelligent characteristics of the holistic intelligent governance theoretical framework reveal the internal relationships among content security risk monitoring and prevention, analysis and assessment, risk dispersion and elimination, and response and disposal after transformation into harmful events, while placing information technology application in a prominent position in terms of implementation means. This full-process and intelligent governance thinking will further clarify the overall work strategy of prevention-first and combination of prevention and treatment, greatly improving the efficiency and effectiveness of network information content ecological security risk governance.

2.3 Significance of Constructing the Holistic Intelligent Governance Theoretical Framework

Through comparative analysis of the construction logic, rationality, and effectiveness of the holistic intelligent governance theoretical framework and its operational characteristics compared with existing governance models, holistic intelligent governance can be considered to place greater emphasis on enhancing the synergy of all governance participants, resource allocation capabilities, information technology intermediary and connecting capabilities, and governance action and objective planning capabilities. The significance of constructing the holistic intelligent governance theoretical framework includes:

2.3.1 Shifting from Problem-Oriented to Goal-Oriented Thinking

Government regulation, multi-stakeholder governance, and network autonomy models generally adopt "problem-oriented" thinking as their basic governance principle. While this principle undoubtedly plays a positive role in addressing currently emerging content ecological security risk hazards or events, the corresponding categorical/dispersed governance strategies targeting specific domains or problems also exhibit utilitarian orientations. The holistic intelligent governance theoretical framework targets the holistic pattern of network information content ecological security environments as its governance objective, using information technology intermediaries to connect holistic and intelligent governance elements. It responds to the overall characteristics of China's network informa-

tion content ecological environment and its hidden risk factors through trend analysis and preventive assessment, rather than being limited to response and disposal after network information content security risk events occur on certain platforms or themes.

2.3.2 Addressing Institutional and Mechanism Barriers in Existing Governance Models

China's government organizational structure follows a two-dimensional fragmentation model. Currently, both government regulation and government-led multi-stakeholder governance models emphasize extensive participation by relevant government departments involving publicity, political-legal affairs, public security, and industry and information technology, supplemented by territorial management principles for network information service platforms. Under this fragmented system, due to departmental interests, "professionalism," and complicated bureaucratic procedures and rules, policy barriers widely exist between "strips" and between "strips" and "blocks," making inter-departmental governance collaboration extremely difficult. Meanwhile, network autonomy models suffer from weakened self-organization of overall network content ecological security due to relevant subjects' profit-driven motivations. The holistic and intelligent governance integrated through information technology as an intermediary can, to some extent, break through these institutional and mechanism barriers and self-organization obstacles.

2.3.3 Emphasizing Modern Information Technology Application

In practice, the three existing governance models often rely heavily on human resource inputs (so-called "internet water armies" exemplify this), with limited breadth and depth of technology application despite some usage. Artificial intelligence technology, big data technology, and others have proven to have broad application potential and prospects in network information content ecological security risk governance practice. Some experts contend that over 90% of massive real-time multimedia content can be accurately identified and filtered by intelligent technology, with mature implementation solutions in natural language processing, image recognition, and voiceprint recognition in the content security domain. Highlighting the role of information technology in the holistic intelligent governance theoretical framework construction can not only improve the effectiveness of content security risk identification and governance but also enable trend-based prevention of security risk evolution dynamics, thereby demonstrating proactive governance thinking.

3 Implementation Strategies for Holistic Intelligent Governance of Network Information Content Ecological Security Risks

The construction of the holistic intelligent governance theoretical framework for network information content ecological security risks embodies the concept of organic fusion of holistic and intelligent governance mediated by information

technology. Its implementation can proceed through the following strategies:

3.1 Establishing an Institutionalized Mechanism Guarantee System

A network information content security risk prevention and control mechanism established on the basis of rule of law is integral to the holistic intelligent governance theoretical framework construction, with rules and institutions being indispensable to any network governance model. The core content of mechanism guarantee system construction includes building a multi-stakeholder collaborative participation network information content risk prevention and control mechanism, a network information content production and distribution incentive and prohibition complementary mechanism, a multi-layer review mechanism for network information content security risks, and a responsibility and relief mechanism for network information content security risks.

3.2 Implementing an Intelligent Technical Support System

Theoretically, big data and related technology applications can enable scientific analysis and prediction of network information content security risk sources, risk factors, and risk trends. Intelligent prediction technologies for network information content ecological security risk events include image recognition technology, digital watermarking technology, text filtering technology, data acquisition technology, protocol analysis technology, data restoration technology, content analysis and filtering technology, and deep learning and intelligent processing technology. Since relevant technologies have achieved good research progress in other disciplines, how to absorb and integrate their application in network information content security risk regulation becomes a practical organizational operation issue.

3.3 Implementing an Ecological Platform Governance System

China's network information content ecological security governance adheres to the approach of "government manages platforms, platforms manage users." Due to resource and technology limitations, the government itself does not possess the capacity for comprehensive governance of network information content ecological security risks, so institutional arrangements highlight the assumption of more obligations and responsibilities by network information content service platforms. How to form and improve the internal content ecological security governance system of service platforms becomes crucial, primarily through: constructing process management systems to manage risk nodes from user registration, account management, information release review, comment review, page ecological management, real-time patrol, emergency response, and network rumor and black industry chain information disposal, thereby ensuring that network information service platforms themselves constitute favorable content ecosystems; building a full-link content security risk control system from account registration, login, user behavior, content release, and logout to implement user profiling and full lifecycle management; and improving internal

platform rule systems to meet governance requirements. These rules typically appear as "user agreements" and "codes of conduct" that users must accept to successfully register accounts. Although these internal rules reflect requirements of network laws, regulations, and norms, they also considerably embody platforms' own interests and demands.

3.4 Constructing a Systematic Content Production and Distribution System

The holistic intelligent governance theoretical framework for content ecological security risks highlights counter-indicative governance of positive and negative information, meaning that governance actions involve not only passive removal of negative information but also active production and distribution of positive information. A proactive content production and distribution system aims to achieve dominance in public opinion fields through active discourse construction. "Discourse" is always connected with social institutions and practices, with discourse structure representing an inherent set of rules that determines the form and content of cognitive behaviors and also determines whether network information content poses security risks. Different types of netizens disseminate their "discourse" into cyberspace based on these "inherent rules," potentially triggering security risks due to rule differences. After user-generated content becomes normalized, whether government agencies and relevant content production departments can proactively conduct content production and distribution and further strengthen distribution intensity determines whether content ecological security risks can be actively prevented and controlled. Therefore, official mainstream media and social media platforms with high user concentration should actively assume responsibility for producing and distributing positive energy-oriented content products, and relevant government departments can also proactively conduct systematic planning of network content themes, regularly evaluate the content distribution status of relevant social media, and implement relevant incentive and penalty measures.

3.5 Establishing a Regular Archival Preservation System

The loss risk of network information content represents a less-noticed aspect of its content ecological security risks. Although scholars have researched network information archival preservation in recent years, they have not approached it from the perspective of network information content security risk regulation, and domestic institutions and mechanisms for regular network information content archival preservation have not yet formed. Conducting panoramic investigations of network information content based on events and themes and timely selective archival preservation can help ensure that major social events and important issues are identified and more completely and truthfully restore the evolution trends of events and issues themselves, thereby forming relatively complete social memory assets. This network information content security risk regulation holds significance for ensuring data asset security and national memory security.

4 Summary and Discussion

In summary, the theoretical framework for holistic intelligent governance of network information content ecological security risks possesses unique internal implications and construction logic. Its governance orientation targets the overall pattern of content ecological security risks, its governance motivation aims to achieve favorable content ecological environment objectives rather than specific risk issues or events, it emphasizes synergistic relationships among actors, technical tools, and rule systems, and highlights the intermediary role of information technology, embodying logical characteristics of holistic and intelligent governance integration. Due to space limitations and the fact that current governance cases still primarily focus on "periodic thematic special actions," "fixed-point 定向 special actions," "large content service platform category actions," and "emergency response special actions," the concepts and framework requirements of holistic intelligent governance have not yet been reflected. Therefore, the scientific validity and effectiveness of this theoretical framework cannot yet be verified through specific cases at this stage, representing a limitation of this study. In subsequent research, the authors will attempt to further verify the necessity, rationality, and feasibility of implementation strategies of the holistic intelligent governance theoretical framework by collecting "counter-example" data or samples from existing practical cases, and promote the concrete implementation of the theoretical framework and implementation strategies through specific pathway design.

References

[1] CARAVELLI J, JONES N. Cybersecurity: threats and responses for government and business[M]. California: ABC-CLIO, 2019.
[2] HE Mingsheng. Concept construction and morphological classification of network content governance[J]. Zhejiang Social Sciences, 2020(9): 64-72.
[3] ZHAO Rongying, YU Bo. Research progress and problem analysis of network information security[J]. Modern Information, 2018, 38(11): 116-122.
[4] LI Yuanli. Criminal law improvement for network data security and citizen personal information protection[J]. Journal of China University of Political Science and Law, 2015(4): 64-78, 159.
[5] ZHI Zhenfeng. Legalization of cybersecurity risks and internet content governance[J]. Reform, 2018(1): 44-46.
[6] HE Mingsheng. Positioning and realistic path of China's network governance[J]. Chinese Social Sciences, 2016(7): 112-119.
[7] ZHOU Yi. Research on action routes for digital heritage preservation[J]. Information Studies: Theory & Application, 2012, 35(4): 15-20.
[8] ZHI Zhenfeng. Institutional exploration for improving network ecological governance effectiveness[J]. Information Security and Communications Privacy, 2020(2): 5-11.
[9] ZHOU Yi, JI Shunquan. Research on constructing a multi-stakeholder collaborative governance model for cyberspace[J]. E-Government, 2016(7):

2-11.
[10] XIE Xinzhou, LI Jialun. Development history of China's internet content management macro policies and basic systems[J]. Journal of Information Resources Management, 2019(3): 41-53.
[11] WANG Ping. Research on information quality assessment of user-generated content from multiple perspectives[M]. Beijing: Science Press, 2020.
[12] ZHU Qinghua. Research and application of user-generated content in the new generation internet environment[M]. Beijing: Science Press, 2014.
[13] SU Xinning. Emergency response intelligence system: theory, technology and practice[M]. Beijing: Science Press, 2019.
[14] WANG Shiwei. On information security, cybersecurity and cyberspace security[J]. Journal of Library Science in China, 2015, 41(3): 72-81.
[15] KIMANI K, ODUOL V, LANGAT K. Cybersecurity challenges for IoT-based smart grid networks[J]. International journal of critical infrastructure protection, 2019, 25(1): 36-49.
[16] MA Feicheng, LI Xiaoyu. Research on the structure and evolution of China's internet content supervision subjects[J]. Journal of the China Society for Scientific and Technical Information, 2014, 33(5): 452-464.
[17] HUANG Ruhua, WEN Fangfang. How to regulate government data under open government data conditions: starting from the international open definition and open government data principles[J]. Information Studies: Theory & Application, 2018, 41(9): 37-44.
[18] HE Mingsheng. Network content governance: information quality supervision based on negative lists[J]. New Horizons, 2018(4): 108-114.
[19] PROVAN K G, KENIS P. Modes of network governance: structure, management, and effectiveness[J]. Journal of public administration research and theory, 2008, 18(2): 229-252.
[20] HÄTTEN M. The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism[J]. Global networks, 2019, 19(3): 329-348.
[21] MA Feicheng, LI Xiaoyu. Research on the structure and evolution of China's internet content supervision subjects[J]. Journal of the China Society for Scientific and Technical Information, 2014, 33(5): 452-464.
[22] DAVIS R E. Auditing information and cybersecurity governance[M]. Los Angeles: CRC Press, 2021.
[23] PARDINI D J, HEINISCH A, PARREIRAS F S. Cybersecurity governance and management for smart grids in Brazilian energy utilities[J]. Journal of information systems and technology management, 2017, 14(3): 385-400.
[24] XU Xin. Western countries' network governance experience and its implications for China[J]. E-Government, 2018(12): 45-53.
[25] QIAN X M, ZHANG J Y. Global cybersecurity governance in the new era: status, dilemma, and development[C]//2020 International conference on materials, control, automation and electrical engineering. Piscataway: IEEE Press, 2020: 41-45.
[26] ZHOU Yi. On the composition and action transformation of network information content governance subjects[J]. E-Government, 2020(12): 41-51.

[27] LARSSON O L. The governmental ity of network governance: collaboration as a new facet of the liberal art of governing[J]. Constellations, 2019, 27(1): 111-126.
[28] YU Jianxing, HUANG Biao. Holistic intelligent governance: interactive integration of public governance innovation and information technology revolution[N]. Guangming Daily, 2020-06-12(11).
[29] ZHU Haoqi. Constructing a full-link content risk control system to solve content security challenges[J]. China Information Security, 2020(2): 73-74.
[30] PERRI 6, DIANA L, KIMBERLY S, et al. Towards holistic governance: the new reform agenda[M]. New York: Palgrave, 2002.
[31] TAN Chenghua. Connotation, logic, and foundational analysis of intelligent governance[J]. Leadership Science, 2019(12): 51-54.
[32] CHEN Chengwen. On risk prevention and control capabilities of municipal social governance[J]. Social Scientist, 2020(8): 15-20.
[33] ZHU Qin. Technological mediation theory: a phenomenological approach to technology ethics[J]. Studies in Philosophy of Science and Technology, 2010(1): 101-106.
[34] WANG Cong. Automated news generation—artificial intelligence is gradually entering the financial field[EB/OL]. [2021-10-21]. http://blog.memect.cn/?p=75.
[35] ZHOU Yi. On the construction of network information content ecological governance mechanisms[J]. Journal of Intelligence, 2020, 36(12): 96-101.
[36] CHEN Tangfa. Research on legal issues of network public expression[M]. Guangzhou: Sun Yat-sen University Press, 2017.
[37] WANG T, ULMER J R, KANNAN K. The textual contents of media reports of information security breaches and profitable short-term investment opportunities[J]. Journal of organizational computing and electronic commerce, 2013, 23(3): 200-223.
[38] YU Minjiang. Holistic intelligent governance: a new social governance model driven by block data[J]. Administrative Tribune, 2020(4): 76-82.
[39] ZHU Haoqi. Constructing a full-link content risk control system to solve content security challenges[J]. China Information Security, 2020(2): 73-74.

Author Contributions:
Zhou Yi: Conceptualization, writing and revision of the manuscript; Zhang Xue: Data collection and organization, partial content revision.

This paper is a research outcome of the National Social Science Fund General Project "Research on the Construction and Implementation of Network Information Content Ecological Security Risk Governance Models" (Project No.: 21BTQ013).

Note: Figure translations are in progress. See original paper for figures.