Security Risk Governance Actions for the Cyberspace Information Content Ecosystem and Their Transformation into Post-Print

Authors: Bai Wenlin, Zhou Yi

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] Summarize and reflect on the current status and deficiencies of security risk governance actions in the network information content ecosystem, and enhance the effectiveness of future governance actions.

[Method/Process] Investigate and sort out the characteristics of the four major governance actions in existing network information content ecosystem security risk governance: "periodic thematic special actions," "targeted fixed-point special actions," "large content service platform-targeted actions," and "emergency response special actions," and benchmark against the "Provisions on the Governance of Network Information Content Ecosystem" to analyze the deficiencies existing in current governance actions across five dimensions: governance objectives, governance subjects, governance objects, governance processes and means, and governance tools.

[Results/Conclusion] Propose a "PDCA-five-dimensional elements" governance action logic for security risks in the network information content ecosystem, as well as upgrade and combination strategies for four types of actions: rights-based campaign-style governance actions, normalized participatory governance actions, constructive agency-based governance actions, and perceptive smart governance actions.

Full Text

Preamble

Volume 66, Issue 5, March 2022
ChinaXiv Collaborative Journal

Governance Actions and Their Transformation for Ecological Security Risks of Network Information Content

Bai Wenlin[1], Zhou Yi[2]
[1] School of Management, Tianjin Normal University, Tianjin 300387
[2] School of Social Science, Soochow University, Suzhou 215123

Abstract:
[Purpose/Significance] This study summarizes and reflects on the current status and deficiencies of governance actions for ecological security risks of network information content, aiming to enhance the effectiveness of future governance actions. [Method/Process] The article investigates and categorizes the characteristics of four major governance actions: "periodical theme-based special actions," "fixed-point targeted special actions," "large content platform-targeted actions," and "emergency response special actions." Benchmarked against the *Regulations on the Ecological Governance of Network Information Content*, it analyzes existing deficiencies in five aspects: governance objectives, governance subjects, governance objects, governance processes and methods, and governance tools. [Result/Conclusion] The article proposes a "PDCA–Five Elements" governance action logic for ecological security risks of network information content, along with four upgraded and combinable action types: rights-based campaign-style governance, normalized participatory governance, constructive active governance, and perception-based smart governance.

Keywords: governance action; network information content ecology; security risk; transformation
Classification Number: G203
DOI: 10.13266/j.issn.0252-3116.2022.05.003

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

Author Biographies: Bai Wenlin, Lecturer; Zhou Yi, Professor and Doctoral Supervisor, Corresponding Author, Email: zhouy@suda.edu.cn.

Received: June 6, 2021; **Revised:** October 31, 2021; **Page Range:** 24-32; **Responsible Editor:** Wang Chuanqing

Bai Wenlin, Zhou Yi. Governance actions and their transformation for ecological security risks of network information content [J]. Library and Information Service, 2022, 66(5): 24-32.

1. Background and Problem Statement

The health of the network ecological environment is closely linked to improvements in people's well-being, the construction of cyber civilization, and the realization of a cyber power strategy. With the continuous development of mobile internet and the evolution of cyberspace, coupled with the low-cost and

low-barrier characteristics of network information production, acquisition, dissemination, and utilization, security risk issues in the network ecosystem have emerged incessantly. In particular, these risks have gradually evolved from traditional cybersecurity issues concerning information systems and network structures toward content-related security risks, including privacy violations, vulgar content, online violence and terrorism, ideological security risks, and intellectual property infringements [1]. Network information content security risks refer to the potential consequences of publishing or disseminating illegal or harmful information. Various forms, contents, and characteristics of such risks collectively constitute the overall security risk problem of the network information content ecosystem. Therefore, governance of security risks in the network information content ecology constitutes an essential component of network information content governance and represents a critical breakthrough for addressing broader network ecological environment issues.

In recent years, China has increasingly strengthened governance of the network ecological environment, focusing particularly on network information content to foster a clean cyberspace. Substantial governance measures have been implemented in three main areas. First, China has enhanced the formulation and promulgation of laws, regulations, and policies. At the national level, laws such as the *National Security Law* and the *Cybersecurity Law* have been enacted, along with the *Regulations on the Ecological Governance of Network Information Content*, which systematically stipulates the governance requirements for the network information content ecosystem. Additionally, policies including the *Methods for Identifying Illegal and Non-compliant Collection and Use of Personal Information by Apps*, the *Cybersecurity Review Measures*, the *Regulations on the Administration of Public Account Information Services for Internet Users*, the *Guiding Opinions on Strengthening the Standardized Management of Online Live Streaming*, the *Regulations on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*, and the *Administrative Measures for Online Live Streaming Marketing (Trial)* have been issued to emphasize control over information content security risks in various cyberspace sub-domains, aiming to achieve comprehensive policy coverage and management of ecological security risks in network information content.

Second, a series of practical governance actions have been carried out, such as the "Clear and Bright" campaign, the "Clean Network" campaign, the "Protect Our Youth" campaign, and the online live streaming platform rectification campaign. According to relevant data, these efforts have achieved certain results in recent years, with substantial numbers of illegal and harmful information items, websites, and accounts being disposed of, leading to overall improvement in the network ecology [2]. However, large amounts of illegal and harmful information still flood cyberspace, creating instability for government operations, enterprise activities, and people's daily lives [3]. Whether existing governance actions adequately reflect the spirit of current policies, whether they are truly effective, and whether areas exist for improvement are pressing questions that require answers. Summarizing and reflecting on the current status and deficiencies of

governance actions for ecological security risks of network information content forms the foundation for enhancing future governance effectiveness.

Current academic research on governance of ecological security risks in network information content primarily focuses on individual risk issues, such as studies on the manifestations, characteristics, impacts, and countermeasures for online rumors, intellectual property rights, and ideological issues [4-6]. This research lacks general and comprehensive understanding of overall patterns and responses to holistic ecological security risks. Moreover, existing studies predominantly concentrate on theoretical discussions of models, pathways, mechanisms, institutions, and technologies [7-13], with few systematic reviews and evaluations of current governance actions. Consequently, the evidentiary basis and targeted nature of proposed governance countermeasures require strengthening. To address this gap, this article systematically reviews the progress of governance actions for ecological security risks of network information content and, benchmarked against the *Regulations on the Ecological Governance of Network Information Content*, summarizes future action logic and strategic transformation directions by analyzing the content, characteristics, and methods of existing governance actions.

---

2. Governance Action Practice and Typological Analysis for Ecological Security Risks of Network Information Content

2.1 Classification of Governance Actions

To comprehensively and targeted understand the current status of China's governance actions for ecological security risks of network information content, this study examines the official website of the Cyberspace Administration of China (http://www.cac.gov.cn/), focusing on all notices, news reports, and summary reports regarding network information content governance from the past three years, particularly since the promulgation of the *Regulations on the Ecological Governance of Network Information Content*. Based on the content and characteristics of each action, the governance actions are broadly categorized into four types: "periodical theme-based special actions," "fixed-point targeted special actions," "large content platform-targeted actions," and "emergency response special actions," as detailed in Table 1 .

Table 1. List of Governance Actions for Ecological Security Risks of Network Information Content

Action Type	Representative Actions
Periodical Theme-Based Special Actions	Clear and Bright Campaign: 2019 Clear and Bright; 2020 Clear and Bright Special Rectification of Minors' Summer Online Environment; 2020 Clear and Bright; 2021 Clear and Bright; 2021 Clear and Bright · Spring Festival Online Environment; 2021 Clear and Bright · Rectifying Online Historical Nihilism; 2021 Clear and Bright · Algorithmic Abuse Governance; 2021 Clear and Bright · Cracking Down on Online Water Armies, Traffic Fraud, and Black PR; 2021 Clear and Bright · Minors' Online Environment Rectification; 2021 Clear and Bright · Rectifying PUSH Pop-up News Issues; 2021 Clear and Bright · Standardizing Website Account Operations; 2021 Clear and Bright · Rectifying Online Entertainment and Hot Ranking ChaosClean Network Campaign: Clean Network 2019; Clean Network 2020; Clean Network 2021Protect Our Youth Campaign: Protect Our Youth 2019; Protect Our Youth 2020; Protect Our Youth 2021Sword Network Campaign: Sword Network 2019; Sword Network 2020; Sword Network 2021
Fixed-Point Targeted Special Actions	Malicious Online Marketing Account Rectification; Online Live Streaming Industry Rectification; APP Rights Infringement Rectification; Minors' Online Course Platform Rectification; Mobile Browser Disruption of Online Communication Order Rectification; Mobile Application Information Content Chaos Rectification; Integrity Deficiency Special Governance; Commercial Website Platforms and "Self-media" Communication Order Issues Centralized Rectification; "Self-media" Basic Management Special Governance; Centralized Rectification of Online "Paid Post Deletion" and "Soft Pornography"; In-depth Promotion of "Knowledge Community Q&A" Governance

Action Type	Representative Actions
Large Content Platform-Targeted Actions	Talks with Phoenix Network; Talks with Baidu; Talks and Penalties with Sina Weibo; Talks with 10 Live Streaming Platforms including Huya and Douyu; Investigation of "@Beijing News Our Video" Weibo Account; Talks with "Xueersi Online School"
Emergency Response Special Actions	Information Epidemic Governance During COVID-19 Pandemic

2.2 Content and Characteristics of Governance Actions

2.2.1 Periodical Theme-Based Special Actions Periodical theme-based special actions are routine, foundational, continuous, and long-term governance initiatives conducted annually, with some traceable to earlier cyberspace governance activities. Current ongoing special actions include the Clear and Bright Campaign, Clean Network Campaign, Protect Our Youth Campaign, and Sword Network Campaign. The Clear and Bright Campaign represents a comprehensive governance action covering all network communication channels and platforms. The Clean Network Campaign is a special action led by the Ministry of Public Security focusing on combating online illegal crimes. The Protect Our Youth Campaign is a special action launched by the National Anti-Pornography and Anti-Illegal Publications Office targeting "pornographic" and "illegal" cases involving minors. The Sword Network Campaign is a joint special action by the National Copyright Administration, Ministry of Industry and Information Technology, Ministry of Public Security, and the Cyberspace Administration of China against online copyright infringement.

These special actions exhibit three main characteristics. First, they involve cyclical and comprehensive governance: special rectification actions are carried out continuously, covering all types of network communication channels and platforms across the entire network, with annual governance consolidating results. The Clear and Bright, Clean Network, Protect Our Youth, and Sword Network campaigns are conducted annually with strong influence and sustainability. Second, they feature localized, top-down proactive governance: these actions implement a top-down governance model from central to local levels. For example, the widely influential Clear and Bright Campaign is led by the national Cyberspace Administration, while local cyberspace administrations also conduct targeted actions, such as Hebei Province's "Clear and Bright • Yanzhao 2020" network ecology governance special action and similar campaigns in Jilin, Yunnan, Gansu, and Xinjiang [14]. Third, governance themes focus on issues severely affecting network ecological security: besides the comprehensive Clear and Bright Campaign, the Clean Network, Protect Our Youth, and Sword Network campaigns target themes—online illegal crimes, minors' "pornographic" and "illegal" cases, and online copyright infringement—that severely threaten

network security.

2.2.2 Fixed-Point Targeted Special Actions These actions target specific segments of cyberspace, including knowledge community platforms, online live streaming platforms, mobile browsers, mobile applications, online course platforms, apps, malicious marketing accounts, self-media, and short videos. They present three main characteristics. First, they employ short-cycle, focused "targeted" governance: these actions typically last between 45 days and 6 months, concentrating efforts on issues strongly reflected by netizens through precise "targeted" governance. Second, they represent passive governance: according to relevant news reports, all fixed-point targeted governance objects are issues that have aroused strong public reaction, with network information authorities primarily relying on public reports and clues—conducting passive governance based on public opinion. Third, they demonstrate exploratory governance: due to the dispersed, complex, and highly concealed nature of current network information content issues, and because authorities have yet to fully grasp the patterns of information content generation and dissemination, governance measures and methods exhibit a "crossing the river by feeling the stones" characteristic. For example, in rectifying online live streaming platforms, relevant authorities are exploring governance measures such as hierarchical classification standards, reward and product promotion rules, and online anchor evaluation systems [15]; regarding self-media disorder, authorities are exploring the construction of self-media credit management systems [16].

2.2.3 Large Content Platform-Targeted Actions Content service platforms provide technical support for network information content dissemination, aggregating massive amounts of content while serving as information hubs for content producers and users [20]. Large content platforms have vast user bases, wide reach, and significant influence, representing powerful mainstream media that largely determine societal value judgments. However, in recent years, many large content platforms have frequently experienced problems, repeatedly exposing issues such as disseminating vulgar information, "clickbait" articles, illegal public opinion during public health emergencies, paid post deletion, soft pornography, and online gambling. In response, the Cyberspace Administration, together with the Ministry of Public Security and other departments, has conducted talks and imposed penalties on these platforms, urging them to abide by legal and moral bottom lines and promote a healthy network space environment.

These actions feature two main characteristics. First, governance objects are all large content platforms: the enterprises subject to talks are all influential platforms, such as Sina, Baidu, Phoenix Network, and Hupu. Second, governance methods combine self-inspection and self-correction with punitive measures: actions primarily urge problematic platforms to conduct self-inspection and self-correction, supplemented by relevant penalties and deadlines for rectification. For example, authorities urged 10 live streaming platforms to centrally rectify vulgar content issues and urged Sina Weibo to rectify disruptions to

online communication order and dissemination of illegal information.

2.2.4 Emergency Response Special Actions Emergency response special actions primarily address public opinion issues arising from natural disasters, safety incidents, and public health emergencies. Information content ecological security problems generated during such events are more complex, rapidly evolving into major public opinion incidents within short timeframes. Issues such as untimely, inaccurate, non-transparent, and false information can trigger social instability. During the COVID-19 outbreak in 2020, the accompanying "information epidemic" in cyberspace reflected such network information ecological problems. Special actions targeting these issues exhibit two characteristics. First, they adopt wartime mechanisms: network regulatory departments at all levels rapidly establish wartime mechanisms, issuing wartime requirements, promptly investigating and dealing with illegal rumors, and releasing accurate information in a timely manner. For example, during the pandemic, major websites set up special columns such as "Epidemic Prevention and Control Rumor Refutation Zones" on their homepages [21]. Second, they establish collaborative work mechanisms: nationwide, top-down special teams for cyberspace governance are rapidly formed, establishing horizontal and vertical collaborative linkage mechanisms responsible for information notification, online patrol law enforcement, and cleanup rectification.

Although the four types of network information content ecological governance actions differ in form and characteristics, they share common features. First, government-led governance: horizontally, core departments such as the Cyberspace Administration, Ministry of Public Security, and National Anti-Pornography and Anti-Illegal Publications Office are the main implementing bodies; vertically, they exhibit top-down control and implementation characteristics. Second, obvious temporary and fragmented governance features: fixed-point targeted governance, content platform talks, and emergency response governance are all temporary control measures targeting specific network information security risk issues, with dispersed governance objects. Even periodical theme-based special actions, while seemingly continuous on the surface, still involve fragmented governance by field and problem during implementation. Third, administrative means dominate: current governance actions primarily employ administrative methods such as talks and penalties, reflecting a control-oriented mindset focused on blocking, cleaning up, and punishing. While current governance actions can relatively quickly focus on major network security risk points and achieve immediate results, their governance objects are relatively limited, their impact scope is small, and they are heavily influenced by government department initiative. They cannot form continuous normalized governance effects nor facilitate the creation of a holistic network information content ecological security environment, necessitating holistic reflection on governance actions.

2.3 Identifying Governance Issues Through Policy Benchmarking

The *Regulations on the Ecological Governance of Network Information Content*, implemented on March 1, 2020, represents an important departmental regulation following the *National Security Law*, the *Cybersecurity Law*, and the *Administrative Measures for Internet Information Services*. To assess the legality and compliance of existing governance actions, this study divides the regulation's text into five elements: governance objectives, governance subjects, governance objects, governance processes, and governance tools. Policy analysis reveals: (1) At the governance objectives level, the regulation emphasizes creating a healthy network ecology, protecting the legitimate rights and interests of citizens, legal persons, and other organizations, and safeguarding national security and public interests. (2) At the governance subjects level, it emphasizes collaborative participation by core actors including government, enterprises, society, industry organizations, and netizens, clarifying their respective rights, responsibilities, and obligations. (3) At the governance objects level, it focuses on strengthening governance of network information content producers, content service platforms, and content service users. (4) At the governance process level, it emphasizes establishing and improving work mechanisms for information sharing, consultation and notification, joint law enforcement, case supervision, information disclosure, inspection, evaluation, and accountability. (5) At the governance tools level, it emphasizes the application of core tools including legal basis, organizational structure, work mechanisms, and technical means.

Benchmarked against these policy essentials and combined with analysis of the four governance action types, several issues warrant attention:

2.3.1 Governance Objectives Require Further Specification Since policies such as the *National Security Law*, *Cybersecurity Law*, *Administrative Measures for Internet Information Services*, and *Regulations on the Ecological Governance of Network Information Content* all set relatively macro-level objectives emphasizing network ecology maintenance and protection of national security, public interests, and legitimate rights and interests, it is crucial to classify and specify governance objectives based on current risk types and response practices.

2.3.2 Multi-Subject Collaborative Mechanisms Require Strengthening Governance cases demonstrate that government departments are the core subjects in network information content ecological security governance. However, governance processes often encounter dilemmas of no one taking responsibility, competing for jurisdiction, inconsistent law enforcement standards, and overlapping repeated enforcement [19]. Government forces in cyberspace remain relatively isolated, fragmented, and decentralized [17-18]. Additionally, enterprises are crucial subjects in network information content ecological security governance, and their self-discipline and fulfillment of responsibilities are key to forming a healthy network information content environment. However, enterprises cannot complete governance tasks alone. For example, a typical

characteristic of current online black and gray industries is cross-platform illegal activities, using cheating and traffic diversion to illegally profit from fake followers and fake traffic. The absence of cross-platform governance currently makes it difficult to effectively address such cross-platform illegal activities [22]. Therefore, cross-platform collaborative mechanisms and online-offline synergistic governance mechanisms require strengthening.

Furthermore, existing policies emphasize collaborative governance among government departments, enterprise platforms, individual netizens, industry organizations, and other social actors. Clarifying the boundaries and collaborative responsibilities of these subjects constitutes a key issue.

2.3.3 Governance Objects Require Further Extension and Deepening First, current governance objects are mostly content service platforms. Network information content ecological security governance objects include three categories: network information content producers, content service platforms, and network information content service users. However, current governance practices primarily target network information content service platforms. While platforms are carriers for network information generation, transmission, and use, this represents partial governance. Only by applying information lifecycle management thinking can governance activities form a holistic situation.

Second, current governance objects are mostly negative information. The *Regulations on the Ecological Governance of Network Information Content* emphasize both rectifying illegal and harmful negative information and encouraging the publication of positive energy information. Current governance actions primarily focus on rectifying negative information, measuring governance performance mainly by the number of illegal and harmful information items cleaned up, illegal accounts disposed of, and illegal platforms shut down. Creating a healthy network ecology requires guiding content producers to actively publish information that aligns with socialist core values, promotes positive energy, and extols truth, goodness, and beauty; guiding content service platforms to recommend healthy, sunny, and positive information; and guiding content users to employ civilized and healthy information. Moreover, governance of more concealed risks such as cross-border data transmission security risks, content manipulation risks, and memory disappearance risks remains insufficient.

Third, current governance actions mostly target information content itself, with less attention paid to the intentions of content publishers, the generation logic and dissemination patterns of illegal and harmful information, or its evolution trends.

2.3.4 Governance Processes and Methods Require Optimization In terms of governance processes, current actions mostly employ temporary, fragmented governance measures targeting specific issues. Although "periodical theme-based special actions" are annual and routine, their implementation also exhibits fragmented characteristics. In terms of governance methods, current

actions primarily employ rigid punitive measures such as suspending sections or functions, suspending new user registration, disposing of responsible persons, ordering rectification within deadlines, blacklisting, and shutdowns, which struggle to create continuous regulatory effects. In terms of governance stages, current actions mainly represent a passive post-event response model, often conducting inspections and urging self-inspection and rectification only after strong public reaction.

2.3.5 Governance Tools Require Further Improvement Theoretically, policy tool elements that can be applied include laws, regulations, and policies; technical means; and organizational mechanisms. While significant progress has been made in laws, regulations, and policies in recent years, many policy gaps remain, such as regarding cross-border data transmission and online violence. In terms of technical means application, current approaches still follow passive governance models of "investigation and screening" and "strike when exposed." The application of intelligent means for proactive risk assessment, early warning, automatic execution, and disposal remains in its infancy. Simultaneously, there is a tendency toward excessive technology application, with frequent occurrences of over-filtering and mis-filtering information [23]. In terms of organizational mechanisms, there is an urgent need to construct an ecological security risk governance community with participation from government, platforms, and citizens.

---

3. Transformation Ideas for Governance Actions for Ecological Security Risks of Network Information Content

Addressing the limitations identified above, this article proposes transformation ideas from two dimensions: governance action logic and governance action pathways.

3.1 Design of "PDCA–Five Elements" Governance Action Logic

Based on the limitations and areas for improvement in current governance actions across the five aspects of governance objectives, subjects, objects, processes, and tools, and considering that governance actions for ecological security risks of network information content require continuous quality control to form virtuous cycles and enhance governance effectiveness, this study designs a "PDCA–Five Elements" governance action logic following the Deming Cycle (Plan-Do-Check-Action) while incorporating all policy elements of governance objectives, subjects, objects, processes, and tools. As shown in Figure 1 [Figure 1: see original paper]:

Figure 1. "PDCA–Five Elements" Governance Action Logic for Ecological Security Risks of Network Information Content

3.1.1 Plan: Governance Action Planning First, conduct legal governance planning by strengthening the planning and formulation of the legal and policy framework for network information content ecological security risk governance, improving the policy basis for governance actions. Priority should be given to policy development for prominent issues such as the concentrated emergence of harmful information and personal privacy leaks, while planning controls for both traditional and new types of illegal and harmful network information, incorporating all stakeholders into policy oversight, establishing platform ecological records and integrity credit systems, and creating multi-dimensional governance rules. Second, conduct holistic governance action objective planning for network information content ecological security risks. The approach of combining routine continuous governance, stage-based thematic governance, and emergency governance should be maintained. Based on a comprehensive understanding of current risk types and characteristics, clarify the direction and focus of risk governance, form measurable governance objectives at all levels, and promote the creation of a healthy network ecological environment. Third, conduct resource allocation planning for network information content ecological security risk governance actions. Beyond conventional resource allocation planning for specialized talent teams and financial resources, strengthen technology resource allocation planning aimed at intelligent governance, particularly systematic planning for artificial intelligence technology, data collection and analysis technology, restoration technology, perception technology, and processing technology. Through technology forecasting, deeply excavate security risks behind data and analyze the root causes and development context of hidden dangers [24].

3.1.2 Do: Governance Action Execution During execution, fully consider the five policy essentials of governance objective establishment, governance subject construction, governance object clarification, scientific governance processes, and governance tool allocation: construct a governance community for network information content ecological security risks, clarifying the responsibilities and obligations of various participating subjects [25]; conduct comprehensive, whole-process governance around the entire information content lifecycle and related stakeholders; implement diversified governance means including legislation, administration, and judiciary; continue strengthening the construction of various collaborative execution mechanisms, linkage operation mechanisms, and online-offline synergistic mechanisms; and enhance the application of smart governance tools for automatic recommendation of positive energy information and automatic identification and filtering of illegal and harmful information.

3.1.3 Check: Governance Action Inspection The inspection stage validates the effectiveness of routine or stage-based special actions and represents an important phase for proposing new issues and directions. Establishing a scientific performance evaluation indicator system for both governance departments and regulated objects is a prerequisite for action inspection. The inspection

process should conduct performance evaluation across three dimensions: pre-action, during-action, and post-action. Indicators such as the number of access qualifications, review quantities, policy planning adaptability, early warning capability, intelligence level, and predictability can be included for pre-action evaluation; quality, emergency response capability, and precision-compliance indicators for during-action evaluation; and social benefits, economic benefits, and plan execution indicators for post-action evaluation. For current governance performance evaluation, focus should be placed on object-labeling governance for both positive and negative information, continuously improving incentive lists, problem lists, and responsible subject lists, and establishing an annual inspection reporting system.

3.1.4 Action: Governance Action Adjustment Governance action adjustment involves correcting existing actions and constitutes a critical link for improving action scientificity and effectiveness. Based on the annual inspection reporting system, improvements should be made to governance planning, processes, objects, and tools, particularly proposing suggestions for policy formulation or revision.

3.2 Upgrading and Combination of Governance Action Types

Addressing current governance action deficiencies and considering the logical design requirements for spiraling upward governance action effectiveness, this study proposes strategies for action upgrading and combination.

3.2.1 Diversified Upgrading of Governance Actions Governance of network information content security risks represents the organic unity of "rule of law, participatory governance, ethical governance, and technological governance" [26]. Based on this, this article proposes four governance action types:

(1) Rule of Law—Rights-Based Campaign-Style Governance Actions. Compared with conventional institutional governance, rights-based campaign-style governance more reflects a control-oriented mindset, emphasizing the state's temporary concentration of social resources through political mobilization and administrative departments using laws, regulations, and policy rules to achieve governance objectives. Its basic characteristics include flexible governance means, integrated resource allocation tendencies, and flattened organizational forms [30]. In network information content ecological security governance, campaign-style governance can rapidly construct an administrative pressure environment through laws, regulations, and policy rules, providing swift responses when conventional governance fails and achieving temporary governance scale and performance improvements. For example, during the initial COVID-19 outbreak, rumors proliferated uncontrollably online, and strong administrative measures could quickly establish a pressure environment to effectively curb illegal rumor-mongering activities. However, its disadvantage lies in being a centralized governance model that does not

align with the decentralized characteristics of network information content and multi-directional information flow patterns. Moreover, the governance process requires segmenting governance objects and scopes, making it suitable only for temporarily alleviating governance pressure and for short-term governance of single issues in specific domains.

(2) Participatory Governance—Normalized Participatory Governance Actions. Normalized participatory governance actions abandon the single governance model of government management departments, emphasizing broad participation by multiple stakeholders in the "source-channel-destination" structural relationship and forming normalized mechanisms. Participatory governance actions constitute important content for modernizing China's governance system and capabilities, effectively improving the political ecological environment, cultivating social capital, and enhancing governance efficiency and effectiveness. However, the difficulty lies in whether the division of responsibilities among participating subjects can be clarified, whether their interests can be coordinated, and whether normalized mechanisms can be sustained.

(3) Ethical Governance—Constructive Active Governance Actions. Constructive active governance actions abandon current lagging, passive governance methods, emphasizing the constraining power of network civilization and ethical cognition on network behavior subjects and emphasizing the proactive, conscious construction of healthy network information content by network behavior subjects, thereby forming the basic social environment for network information content governance. Ethical governance possesses basic functions of constraint, education, influence, and guidance, serving as an effective supplement to the relatively rigid means of rule of law. However, the difficulty lies in its nature as a consciousness control method that must rely on certain procedures and rules and long-term influence to form specific self-governance.

(4) Technological Governance—Perception-Based Smart Governance Actions. Perception-based smart governance actions represent the integration of technology and governance subjects, emphasizing the construction of an effective control system based on technological support. Through technological means, governance methods and processes become more precise and humanized, thereby enhancing data resource integration and complex business processing capabilities [28]. In the dilemma of passive and inefficient human governance, technologies in technological governance such as intelligent perception, detection, identification, and control undoubtedly greatly enhance holistic perception capability of networks [29], enabling early and accurate identification at the source, timely blocking during dissemination, and early warning and effective response before results occur, significantly improving governance efficiency and effectiveness [27]. However, the difficulty lies in the need to embed governance rules and ethics as constraints during technological development, and the accuracy of perception and judgment depends on technological advancement.

3.2.2 Synergistic Combination of Governance Actions (1) Upholding the Organic Unity of Rule of Law, Participatory Governance, Ethical Governance, and Technological Governance. As analyzed above, the four governance types fully consider the needs and characteristics of various complex governance scenarios, accommodating the allocation of various governance tools and the scientific nature of governance methods. Under the comprehensive governance objective of network information content ecological risk security, the four governance action types must achieve comprehensive organic unity, combining normalized governance with rights-based governance, proactive governance with passive governance, and rigid means with flexible means. This approach mobilizes the enthusiasm of all stakeholders, achieves rational optimization and allocation of effective resources, and leverages strengths while avoiding weaknesses to form good comprehensive governance benefits.

(2) Employing Different Governance Action Combinations for Different Stages, Nature, and Influence Levels of Security Risks. Security risk governance cannot adopt a one-size-fits-all approach. Based on risk characteristics and patterns and following governance principles of "targeting, economy, and effectiveness," different governance action strategies should be employed for different security risks to achieve good governance effects while maximizing cost savings. Specifically, this can be approached from three dimensions:

First, different governance action combinations for different development stages of security risks. Referencing network information lifecycle development patterns and public opinion diffusion patterns [31], combined with risk management process theories, this study proposes dividing network information content ecological security risks into four stages: risk gestation initial stage, risk dissemination and diffusion stage, risk continuous fermentation stage, and risk decline stage. The risk gestation initial stage features variability, concealment, and weak impact, leading to difficulties in source identification, characterization, and impact estimation. However, its contingency, singularity, and weak characteristics make governance relatively easy, allowing the use of ethical and technological governance actions to achieve risk avoidance. For example, localized vulgar content risks in network spaces can be effectively controlled through intelligent post deletion and platform education warnings. The risk dissemination and diffusion stage features risks gradually spreading in cyberspace, leading to partial group risks. At this stage, partial group risk characteristics become clear, and different attitudes and positions exist in cyberspace. Therefore, ethical and participatory governance means are recommended to guide risks toward attitudes and positions that align with socialist core values, promote positive energy, and extol truth, goodness, and beauty, effectively achieving risk transfer. For example, regarding the ideological risk of "lying flat" (a passive lifestyle attitude), authoritative media, online influencers, and the public can be guided to speak out about the dangers of ideological inertia, guiding the public to cultivate enterprising spirits. The risk continuous fermentation stage features risks forming large-scale group effects under ineffective guidance, potentially causing significant harm to national, social, and people's security. At this stage, stronger

rule of law and compulsory technological governance means should be employed, supplemented by participatory and ethical governance means, to eliminate security risks as quickly as possible. For example, once online terrorism risks emerge online, they can significantly impact public safety, social emotions, and social order, requiring immediate government investigation and intervention to rapidly eliminate risks. The risk decline stage features risks gradually decreasing after implementing a series of governance actions and measures. At this stage, flexible ethical and technological governance means are recommended for mopping-up work to completely eliminate risks.

Second, different governance action combinations for different natures of security risks. The content characteristics and impact scope of security risks should be comprehensively considered to construct a security risk classification system. For risks such as online ideology, historical nihilism, content vulgarization, and network cultural security risks, ethical and participatory governance actions should be strengthened, with rule of law actions applied as appropriate depending on development trends, while technological governance for intelligent judgment and processing should be maintained throughout. For information content security risks involving illegal crimes, online terrorism, and public order disruption, rule of law actions should dominate, combined with the other three governance actions.

Third, different governance action combinations for different influence levels of security risks. The influencing factors of security risks, including subjects, objects, content, and environment, should be comprehensively considered to construct a risk assessment model and establish a security risk grading system. Risks should be classified into especially major risks, major risks, serious risks, and general risks based on influence, with different governance actions employed for different hazard and influence levels. The greater the risk impact and harm, the higher the governance level, and the more governance means should be dominated by rule of law, supplemented by ethical governance, while incorporating technological and participatory governance throughout.

Conclusion

The *Regulations on the Ecological Governance of Network Information Content* clarifies the core essentials of network information content governance across five aspects: governance objectives, subjects, objects, processes, and tools. Existing governance action practices have responded well to the policy in some respects but also exhibit areas for improvement. This article proposes deepening the implementation requirements across these five aspects, combining unified and rational planning, effective execution, rigorous inspection, and timely adjustment to construct a governance action logic for enhancing network information content ecological security risk governance. It further proposes scientific upgrading of four governance action types—rule of law, participatory governance, ethical gov-

ernance, and technological governance—and their combination strategies. This study overcomes existing research limitations that focus on individual, specific network information content risk countermeasures and lack systematic review, reflection, and evaluation of current governance actions, providing holistic response ideas for network information content ecological security risk governance. Future research will continue to conduct empirical investigations and applications of the proposed response ideas to further adjust relevant implementation strategies.

References

[1] *Regulations on the Ecological Governance of Network Information Content* Achieves Results in Website Platform Self-Inspection and Self-Correction [EB/OL]. [2021-03-23]. https://baijiahao.baidu.com/s?id=1670884092852266610&wfr=spider&for=pc.

[2] National Cyberspace Administration's 2020 Governance Action Overview [EB/OL]. [2021-03-23]. http://yuqing.people.com.cn/n1/2021/0114/c209043-31999568.html.

[3] Zhou Yi. On the Construction of Network Information Content Ecological Governance Mechanisms [J]. Journal of Intelligence, 2020, 39(12): 100-105.

[4] LIAROPOULOS A N. Cyberspace governance and state sovereignty [J]. Computer Law & Security Review, 2020, 36: 105454.

[5] CHU W, LEE K T, LUO W, et al. Predicting the security threats of internet rumors and spread of false information based on sociological principle [J]. Computers & Standards & Interfaces, 2020, 73: 103454.

[6] Liu Zhangyi. Prevention of Network Ideological Risks in the Context of Short Video Rise [J]. Leadership Science, 2020(14): 38-41.

[7] Xie Xinzhou, Zhu Kuangying. Research on Development Trends and Response Strategies of Network Content Governance [J]. News and Writing, 2020(4): 78-84.

[8] Zhou Yi. Network Information Content Governance from the Perspective of Overall National Security: Progress, Connotation and Research Logic [J]. Information Studies: Theory & Application, 2020, 43(8): 44-50.

[9] Song Jiageng, Zhao Lumin, Zhang Yuer. Analysis of Network Supervision Mechanism from the Perspective of Network Governance [J]. Publishing Research, 2020(5): 52-58.

[10] 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.

[11] 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.

[12] LARSSON O L. The governmentalization of network governance: collaboration as a new facet of the liberal art of governing [J]. Constellations, 2019, 27(1): 111-126.

[13] In-depth Development of 2020 "Clear and Bright" Special Actions by Local Cyberspace Administrations [EB/OL]. [2021-04-26]. http://www.cac.gov.cn/2020-07/09/c_{1595854510933390}.htm.

[14] 8 Departments: Research and Formulate Hierarchical Classification Management Standards for Anchor Accounts to Regulate Anchor Sales Behavior [EB/OL]. [2021-04-26]. https://baijiahao.baidu.com/s?id=1674064891608883013&wfr=spider&for=pc.

[15] National Cyberspace Administration Launches "Self-media" Basic Management Special Governance [EB/OL]. [2021-04-22]. https://baijiahao.baidu.com/s?id=1673567752407975617&wfr

[16] Chen Luying. Research on Platform Responsibility in Internet Content Governance [J]. Publishing Research, 2020(6): 12-18.

[17] Zhejiang Launches "Clear and Bright Hero in Action" Campaign to Weave a Dense Network for Epidemic Prevention and Control Ecological Governance [EB/OL]. [2021-02-26]. http://www.cac.gov.cn/2020-03/30/c_{1587116320391779}.htm.

[18] China's Network Ecological Governance Achieves Results [EB/OL]. [2021-03-26]. https://baijiahao.baidu.com/s?id=1671068819583158676&wfr=spider&for=pc.

[19] Shanghai Establishes Comprehensive Coordination and Disposal Mechanism for Major Network Events [EB/OL]. [2021-03-26]. http://www.whb.cn/zhuzhan/cs/20190531/267169.htm

[20] Gui Changni. New Situations and Challenges Facing China's Network Content Governance [J]. China Information Security, 2020(2): 59-62.

[21] In-depth Governance of Online Black and Gray Industries Should Construct Platform Collaborative Linkage Mechanisms [EB/OL]. [2021-04-26]. https://baijiahao.baidu.com/s?id=1671715491717410316&wfr=spider&for=pc.

[22] Wang Lina. Research on the Legalization Transformation of Internet Campaign-Style Governance [D]. Changsha: Hunan Normal University, 2020.

[23] Hu Ling. Website Governance: Institutions and Models [J]. Peking University Law Review, 2009(2): 182-202.

[24] Lin Aichen, Zhang Mengtian. Regulation of Multi-Subject Responsibilities in Network Content Ecological Governance [J]. Journalism Lover, 2021(4): 14-16.

[25] Zhou Yi. On the Composition and Action Transformation of Network Information Content Governance Subjects [J]. E-Government, 2020(12): 41-51.

[26] Jiao Junfeng, Li Xiaodong. The Governance Path for Network Security: Integration of "Technological Governance, Rule of Law, Participatory Governance, and Ethical Governance" [EB/OL]. [2021-05-11]. https://www.thepaper.cn/newsDetail_{{{forward}}}_{{5418485}}}.

[27] Pan Zequan, Ren Jie. From Campaign-Style Governance to Normalized Governance: China's Practice of Grassroots Social Governance Transformation [J]. Journal of Hunan University (Social Sciences), 2020, 34(3): 110-116.

[28] Gil O, Cortés-Cediel M E, Cantador I. Citizen participation and the rise of digital media platforms in smart governance and smart cities [J]. International Journal of E-Planning Research (IJEPR), 2019, 8(1): 19-34.

[29] Chang L Y C, Grabosky P. The governance of cyberspace [M]//Drahos P. Regulatory theory: foundations and applications. Canberra: ANU Press, 2017: 533-551.

[30] Zhou Yi. Network Information Content Governance from the Perspective of Overall National Security: Progress, Connotation and Research Logic [J]. Information Studies: Theory & Application, 2020, 43(8): 44-50.

[31] Shi Cui. Research on the Influence and Governance Path of Micro-Communication Public Opinion [J]. Journal of News Research, 2017, 8(15): 26-27, 39.

Author Contributions:
Bai Wenlin: Participated in formulating research questions and proposing research ideas, collected and analyzed data, and wrote and revised the paper.
Zhou Yi: Formulated research questions, proposed research ideas, wrote and revised the paper, and finalized the manuscript.

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