Network Information Content Ecological Security Risks: Connotation, Types, Causes, and Impacts (Postprint)

Authors: Li Jie, Zhou Yi

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

Abstract

[Purpose/Significance] This study conducts conceptual definition, type classification, analysis of typical risk causes, and inter-risk impact relationships for security risks in the network information content ecosystem, aiming to provide analytical foundations for research on the governance of network information content ecosystem security.

[Method/Process] By summarizing continuously emerging security risks in the network information content ecosystem and integrating national concerns regarding network information security risk prevention, control, and governance, this paper analyzes the types of security risks in the network information content ecosystem. From a holistic perspective of network information ecosystem security risks, it examines the connotations and causes of mainstream and typical risk types, summarizes the overall characteristics of security risks in the network information content ecosystem, and comprehensively analyzes the potential impacts of overall security risks from the perspective of relationships between specific types of network information content ecosystem security risks and the overall risk.

[Results/Conclusion] Security risks in the network information content ecosystem constitute a core component of network information ecosystem security risks. Various types of network information content ecosystem security risks have different causes, yet exhibit overlapping characteristics and impacts. Ensuring the security of the network information content ecosystem requires specifically addressing different types of network information content ecosystem security risks while comprehensively considering their holistic risk impacts.

Full Text

Preamble

Volume 66, Issue 5, March 2022
ChinaXiv Partner Journal

Online Information Content Ecosystem Security Risks: Connotation, Types, Causes, and Impacts

Li Jie, Zhou Yi
School of Sociology, Soochow University, Suzhou 215123

Abstract:
[**Purpose/Significance**] This study defines the concept, classifies the types, analyzes the causes of typical risks, and examines the interrelationships of impacts among online information content ecosystem security risks, aiming to provide an analytical foundation for research on the governance of online information content ecosystem security. [**Method/Process**] Through a systematic review of continuously emerging online information content ecosystem security risks, and in conjunction with national concerns regarding prevention, control, and governance of online information security risks, this paper analyzes the types of online information content ecosystem security risks. From a holistic perspective of online information ecosystem security risks, it examines the connotation and causes of mainstream and typical risk types, summarizes the overall characteristics of online information content ecosystem security risks, and comprehensively analyzes the potential impacts of overall security risks from the perspective of relationships between specific types of online information content ecosystem security risks and the overall risk landscape. [**Result/Conclusion**] Online information content ecosystem security risks constitute the core component of online information ecosystem security risks. While various types of online information content ecosystem security risks have different causes, they overlap in characteristics and impacts. Ensuring the security of online information content ecosystems requires targeted responses to different types of risks while comprehensively considering their overall impacts.

Keywords: online information content ecosystem; ecological security risk; risk types; risk impacts
Classification Number: D631
DOI: 10.13266/j.issn.0252-3116.2022.05.001

---

1. Introduction

As a driving wheel and wing of socialist cyberspace governance with Chinese characteristics in the internet era [1], "cybersecurity" represents one of the core concepts in General Secretary Xi Jinping's strategy for building China into a cyber powerhouse. In practicing contemporary Chinese socialist national security,

China must not only focus on traditional security but also attach importance to non-traditional security domains such as cybersecurity and ecological security, breaking through subject-oriented thinking paradigms to adopt an ecological perspective [2] and focus on cyberspace ecological security. With the rapid development of mobile internet and information technology, risk hazards in cyberspace ecological security continuously extend from cyberspace to the real world. Particularly, the low-cost and low-barrier advantages of online information production, dissemination, and usage, combined with the hidden or difficult-to-control gray zones in cyberspace, have led to a continuous increase in cyberspace ecological security risks triggered by online information content. According to Article 12 of the *Cybersecurity Law of the People's Republic of China* [3], Article 6 of the *Regulations on the Governance of Online Information Content Ecology* [4], and Article 15 of the *Administrative Measures for Internet Information Services* [5], activities that endanger state power, unity, honor, and interests, or ethnic unity; disseminate obscene, pornographic, gambling, violent, murderous, terrorist, or rumor-based content; infringe upon others' privacy and other legitimate rights and interests; and emerging risks such as data memory disappearance and information content manipulation all constitute key focal points for online information content security risk prevention and the critical challenges for online information content security governance. Based on existing regulations, policies, and research findings, this study employs literature analysis and case study methods to investigate issues related to online information content ecosystem security risks. From an ecological thinking perspective, it analyzes the connotation of online information content ecosystem security risks, examines typical risk types including online ideological security risks, online information content vulgarization, online information content manipulation risks, online intellectual property risks, and memory disappearance risks, and provides a holistic analysis of the interactions among these risks.

2. Connotation of Online Information Content Ecosystem Security Risks

Based on the premise that "information is the fundamental element of cyberspace," cybersecurity is essentially about the security of online information content [6]. Online information content security emphasizes selective blocking of information flowing within networks to ensure controllability over information flow [7]. The objects being blocked are various threats identifiable through information content itself. From this perspective, online information content security risks are closely related to information security risks. According to ISO 31000's definition of risk [8]—"risk is the effect of uncertainty on objectives"—online information content security risks can be viewed as uncertain factors affecting the selective blocking of information flow within networks. From an ecological perspective, cyberspace security primarily involves the information domain (characteristics of information content itself), the social domain (im-

pact of cyberspace on real society) [2], the physical domain (hardware equipment in information space), and the cognitive domain (impact of information dissemination on individual thoughts and behaviors). Online information content security, however, emphasizes the information domain and the radiation domain (impacts of information content on national, social, economic, cultural, and network environments). Online information content ecosystem security risks mainly constitute threats to both the information domain and the radiation domain. To understand the connotation of online information content ecosystem security risks, two main threads should be considered: first, these risks are triggered by online information content; second, they require holistic analysis of both the information domain and the radiation domain.

From the perspective of sources and subject evolution, online information content ecosystem security risks primarily originate from defects within the information domain and network internals, involving threats to information systems, network structures, and the security of online information content itself [9]. As the network environment evolves, sources of online information content security risks increasingly manifest in new forms. Beyond traditional risk subjects such as hostile forces, terrorist organizations, commercial spies, organized criminal groups, premeditated individuals (e.g., hackers), and accidental or non-compliant operations by authorized users, various role-players across network content layers have become primary risk subjects. These include online information content producers, disseminators, service providers (including platforms and third-party agencies), and recipients (i.e., users), forming a diverse array of risk subjects in the online information content ecosystem.

From the perspective of specific object manifestations, online information content ecosystem security risk objects include security events that threaten the information domain and radiation domain, as well as the resulting losses within the radiation scope. From an environmental change perspective, innovations in connection devices, media tools, system technologies, service technologies, data technologies, and communication technologies that support cyberspace also provide enabling channels for online information content ecosystem security risks. Under the advantages of network decentralization, efficient interconnectivity, low barriers, easy anonymity, strong binding, and high sharing, risk objects in the online information content ecosystem are more prone to derivation and evolution. Additionally, fragmentation of existing online information content security technologies and technological gaps for emerging risks provide opportunities for risk subjects to exploit security vulnerabilities. Moreover, institutional fragmentation in monitoring and controlling online information content ecosystem security and the absence of relevant policies and regulations create further opportunities. As cyberspace becomes the primary battlefield for future competition, cultural invasion in the online information content ecosystem intensifies, and ideological competition becomes increasingly evident, continuously escalating environmental domain influences on online information content ecosystem security risks.

Overall, the information domain and radiation domain of online information content ecosystem security risks catalyze the subject, object, and environmental elements of these risks. Risk subjects affect information flow, thereby creating security blockages and damage to information content itself, information content systems, and the information content ecological environment.

---

3. Classification of Online Information Content Ecosystem Security Risk Types

In recent years, the state has particularly emphasized prevention and governance of online information security risks in several key areas: (1) Online information security issues concerning state power and sovereignty security. In the current international environment, Western countries led by the United States engage in smearing, slandering, interest inducement, cultural diversion, discourse suppression, and other forms of infiltration and incitement against China's ideology through cultural intrusion, online public opinion, and ideological dimensions. This has long been a point of contention in cyberspace governance and a particularly important security concern for the state. (2) New types of cybercrime concerning people's vital interests, such as online pornography, vulgar hype, online verbal garbage, cyber violence, cyber terrorism, false information, online pyramid schemes, telecom and online fraud, online predatory lending, online "pig butchering" scams, information-based market manipulation, and other cybercrimes. These issues have victimized countless citizens, generated strong social reactions, and severely impacted state stability and government credibility. (3) Big data security risks and governance issues, focusing on data storage, data property rights, citizen privacy, data damage, and data theft.

Based on these national concerns and relevant provisions in the *Cybersecurity Law of the People's Republic of China*, *Regulations on the Governance of Online Information Content Ecology*, and *Administrative Measures for Internet Information Services*, this study classifies online information content ecosystem security risks according to their information domain and radiation domain into the following categories:

3.1 Superstructure-Related Risks

Yang Wenhua et al. [14] argue that network development intensifies threats to national ideology, and the proliferation of cultural products and abuse of cultural rights severely erode superstructure-level security in cyberspace. According to relevant provisions in the *Regulations on the Governance of Online Information Content Ecology*, Article 12 of the *Cybersecurity Law* [3], and Article 15 of the *Administrative Measures for Internet Information Services* [4, 5], this risk type primarily refers to security issues and damages concerning state power, sovereignty, unity, system, ethnicity, and religion that conflict with China's

mainstream ideology and political values, triggered by online information content.

3.2 Property-Related Information Content Risks

Chen Wei et al. [15] analyze new cybersecurity risks under the "four new economies," identifying online pyramid schemes, online fraud, and virtual currencies as major emerging risks. Combined with recent priorities in financial risk prevention [16], property-related information content risks mainly include security issues and damages such as online pyramid schemes, online fraud, online predatory lending, online "pig butchering" scams, online theft, and information-based market manipulation.

3.3 Rights Infringement Risks, such as Intellectual Property Risks

Li Yufeng et al. [17] view intellectual property risks as inevitable "byproducts" of platform economy development under the internet, including security issues and damages such as online piracy, online plagiarism, and unauthorized dissemination. Other examples include security problems and damages from infringing upon netizens' personal privacy, reputation, and other legitimate rights and interests.

3.4 Risks Related to Cyber Cultural Environment Destruction

According to Gui Changni's [18] analysis of new situations in China's online content governance, the online water army problem has become a global challenge. With the blurring boundaries between audiences and disseminators brought by new online media, the anomie of cyber culture reflected by vulgarization of online media content is intensifying [19]. Based on interpretations of the *Regulations on the Governance of Online Information Content Ecology* [20] and Article 15 of the *Administrative Measures for Internet Information Services*, this category includes lowbrow content security issues and damages such as online pornography, online verbal garbage, online hype, online discrimination, and online sensationalism.

3.5 Risks Related to Online Information Content Memory

C. L. Liew et al. [21] argue that memory institutions' use of social media has not prevented or mitigated threats to memory construction. Internet and social media development has increased both advantages for social memory construction and risks for memory deconstruction. Digital memory faces growing risks [22], such as security issues and damages from online information loss, damage, destruction, and non-preservation that cause memory disappearance.

Additionally, there are cybercrime-related risks, such as online gambling, online drugs, and cyber terrorism related to drugs, poison, and terrorism. Overall, although various types of online information content ecosystem security risks

have different emphases, they all exhibit characteristics of diverse variant manifestations, multi-scenario involvement, enhanced security confrontation, and increased camouflage and concealment methods as they evolve with cyberspace depth. On one hand, scenarios such as Western cultural infiltration, online fraud, unauthorized dissemination, content vulgarization, and digital memory disappearance have become normalized threats. On the other hand, as scenarios evolve and security confrontation methods develop, various risk types generate massive amounts of risk content data [23], with variants continuously increasing across text, images, audio, and video. Moreover, as camouflage and concealment methods multiply, security confrontation intensifies [24], making governance of various risk types increasingly urgent.

---

4. Causes of Typical Online Information Content Ecosystem Security Risks

The online information content ecosystem security risk system involves different risk types from various perspectives. Through literature review, this paper summarizes typical risks. Given the numerous subcategories across risk types, it is impossible to exhaustively cover all specific risk content. Therefore, based on needs for extended research, this paper provides brief introductions and cause analyses of typical normalized and emerging risks across different types to serve as references for subsequent analyses of other specific risks. The selected typical online information content ecosystem security risks include: online ideological security risk reflecting superstructure risks; information manipulation risk reflecting new property infringement methods; online information content vulgarization risk reflecting cyber cultural environment destruction; intellectual property risk reflecting piracy, plagiarism, and unauthorized dissemination related to online copyright, data property rights, and online dissemination rights; and online memory disappearance risk reflecting data and information loss, dissolution, and fragmentation.

4.1 Online Ideological Security Risk and Its Causes

Online ideological security risk falls within the superstructure category of online information content ecosystem security risks. It refers to threats in cyberspace that endanger, undermine, or corrode socialist spiritual civilization, historical culture, ideological morality, and value systems—content representing ideology—driven by online information content. Fundamentally, it involves infringements upon national honor, interests, unity, political power, sovereignty, systems, ethnicity, and religion through manipulation of online information values. Systematically, online information content ideological security risk occupies the primary position in the online information ecosystem security risk hierarchy. Only by achieving ideological security can national interest security and security for all netizens' online activities be ensured. Typical risk content includes

de-ideologization, politicization of sensitive events, color revolutions, stigmatization of national image, and inferiority of political systems.

Online ideological security risk is primarily driven by internal and external threats to online information content ecosystem security: (1) **Internal threats**: Ideological pluralism disputes weaken mainstream online ideology. Unlike traditional media-led public opinion guidance centered on news reporting, new online media technologies and platforms provide breeding grounds for diverse values. On one hand, netizens' confidence in mainstream ideology is insufficient, with increased self-negation and evident de-ideologization trends. On the other hand, mainstream online ideology's dominance in public opinion fields has declined, while netizens and civilian media's ability to manipulate opinion orientation has increased. The frequency of sudden social events escalating into ideological debates continues to rise, with clear tendencies for ideological disputes to transform into political events. Leveraging networks' interconnectivity, interactive openness, instant anonymity, and circle-based dissemination characteristics, netizens' "collective voice" in hard-to-regulate areas can easily gather "online popular sentiment," leading to different online ideological disputes, particularly becoming battlegrounds for political viewpoints. This enables non-mainstream online ideologies to compete with mainstream ideology, posing risks of impact and dissolution. The Occupy Central incident, with its sovereignty-undermining discourse and separatist forces' manipulation of Hong Kong residents' values and smearing of China's socialist system, exemplifies this. (2) **External threats**: Foreign ideologies impact China's mainstream ideology. Western hostile forces exploit network freedom to continuously input their cultural values and political system concepts, cultivating agents for hostile ideology input and centrifugal groups within socialism. They organize "color revolution" forces, Falun Gong practitioners, religious extremists, and system deniers to infiltrate online public opinion fields, disseminating information that endangers national security through continuous distortion of history, stigmatization, interest inducement, sugar-coated shells, international marginalization, and event incitement, tearing social consensus apart. Additionally, leveraging globalization advantages, Western cultural neocolonialism centered on Western discourse is evident. Based on inherent imbalances in communication resources between Western and non-Western countries, hostile Western forces exploit networks' cultural penetration, expansion, and transmission advantages. Against backgrounds of increased global ideological collisions and conflicts, they use their cultural hegemony to promote self-perceived superior values under their ideology, targeting China's relatively weak international discourse system to amplify social contradictions and disrupt online public opinion environments. Examples include "rehabilitating" historical figures like Zhou Bapi [25], demonizing Chinese dama (middle-aged women) as a socialist system group [26], guiding and amplifying consciousness of Chinese inferiority ("China's air is poisonous, America's air is sweet") [27], and using Chinese characters in films and games to instill Western superiority.

4.2 Online Information Content Vulgarization Risk and Its Causes

Online information content vulgarization risk affects the overall online atmosphere of online information ecosystem security, representing an environmental threat component. Compared with popularization and refinement of online information content, vulgarization refers to trends where online information content reflects lowbrow, vulgar, and kitschy cyber culture, mixing pornographic, harmful, and misleading content that negatively impacts the online information ecosystem and netizens' physical and mental health [28].

Online information content vulgarization risk is primarily driven by: (1) **Vulgarization of online information content language**: According to the *Online Vulgar Language Investigation Report* [29], emotional venting, malicious slander, and using vulgar content as personalization have triggered online vulgar language including online abuse, verbal violence, and crude expressions such as black slang, profanity, obscene language, and anatomical insults like "piaobazi," "guncu," "jiaoshou," "lvchabiao," "diaosi," and harsh words targeting "black five categories"—urban management officers, doctors, police, experts, and officials. (2) **Vulgarization of online information content media dissemination**: Typical examples include online media, novels, jokes, livestreams, short videos, films, ad links, and bullet comments under the guise of pornography, abuse, or verbal violence, such as livestreams soliciting red envelopes through dangerous actions or fights, and online videos promoting "entertainment 至死, just play." (3) **Vulgar utilization of online information content**: Common practices include using online pornography, verbal violence, spoofs, and crude language pollution for information push, profit, sensationalism, and attention attraction, such as streaming platforms, dark webs, and rented servers profiting from sexual behavior, nudity, and similar video, audio, and image content.

4.3 Information Manipulation Risk and Its Causes

Information manipulation risk refers, on one hand, to information-based market manipulation risk—using information to manipulate markets [30]—generally involving manipulators using information advantages for continuous market transaction manipulation, 偏向 capital manipulation. On the other hand, it refers to online water armies, online pushers, and other interest groups or individuals who, for economic, public opinion, political, or other purposes, use information to incite public sentiment or create social contradictions, belonging to online information content manipulation risk. Essentially, it involves organized, planned, and premeditated actions to obtain benefits or achieve goals through misleading, incorrect, inciting, or exclusive online information. Information manipulation risk includes both threats to online markets and threats to online public opinion environments and other elements for specific purposes, representing property and rights infringement risks in the overall online information ecosystem security risk landscape, with characteristics of capital orientation, concealment, organization, interest-driven motives, and diffusion.

Information manipulation risk is primarily driven by: (1) **Various improper profit-driven behaviors led by online pushers and online haters**: These include improper profit-making through online pushers and haters, and non-legitimate capital behaviors using online information to manipulate stocks and securities, affecting market transactions. Typical examples include "viral marketing," "hype marketing," search engines' "bid ranking," online stock market miracles, online financial scams, the "Xu Xiang case" [31], and online defamation. (2) **Online public opinion manipulation by online water armies and commentators**: To gain attention, guide public opinion, or incite public sentiment polls, online information disseminators pre-plan event topics and use online media for widespread dissemination to occupy public opinion high ground, such as posting inflammatory negative information and false statements under anonymous ordinary netizen identities, especially leveraging sudden events. The "Occupy Central" incident, distorted by separatist forces, exemplifies this. (3) **Cyberspace manipulation threats through advanced technologies like deepfakes**: With artificial intelligence technologies such as generative adversarial networks and cognitive computing, increasingly sophisticated deepfakes are used for online information content manipulation, creating difficulties for intervention (e.g., deep detection of false information). False information manufacturing and dissemination no longer remain at individual and organizational levels; international digital espionage, online content attacks, and digital sovereignty competition continuously emerge, with cyberspace "Balkanization" becoming increasingly apparent.

4.4 Intellectual Property Security Risk and Its Causes

Intellectual property security risk in cyberspace refers to various security issues arising from unauthorized legitimate use, dissemination, or profit-making of digital information content with intellectual property rights during network propagation and usage, such as copyright infringement and online copyright violations of multimedia works, digital products, databases, computer software, and network domains (China's *Copyright Law* Article 57 stipulates that copyright is authorship rights), online patent infringement, and online trademark infringement [32-33]. This represents a rights infringement risk in the overall online information ecosystem security risk landscape. Generally, open-access or freely downloadable online information resources belong to free-use categories, while paid or non-commercial online information resources belong to limited-use categories. Improper knowledge acquisition and dissemination beyond these categories create intellectual property security threats.

Intellectual property security risk is primarily driven by: (1) **Infringing use of online information content**: This includes infringement acts without permission from online copyright, patent, or trademark holders or without legitimate use, such as completely copying online information content—typified by online sales of infringing counterfeit goods, trademark misappropriation, and patent misappropriation (e.g., e-commerce platforms' "same-style" product

imitations)—or slightly modifying content while severely damaging the copyright, trademark, and patent rights of plagiarized information, manifested as plagiarism, tampering, editing, and other improper dissemination or profit-making of digital products, such as uploading, downloading, or reposting others' digital information products without permission or citation, tampering data, plagiarizing webpages, and using illegal hyperlinks [34]. (2) **Infringing dissemination of online information content**: Without statutory licensing or fair use, unauthorized public or illegal dissemination of others' digital information products without authorization from online trademark, copyright, or patent holders, such as illegal dissemination through pirated links, cloud drives, cracked versions, or platform vulnerabilities.

4.5 Online Memory Disappearance Risk and Its Causes

From the perspective of its relationship with overall online information ecosystem security risks, online information memory disappearance risk is a user-perspective risk type. Online information content memory and forgetting are unconscious processes influenced by online information storage technologies, management and norms, storage awareness, memory media, user memory construction systems, and characteristics of online information content. Threats such as memory loss, dissolution, and fragmentation caused by these elements constitute online information memory disappearance risk [35].

Online memory disappearance risk is primarily driven by: (1) **Online information content memory loss**: On one hand, loss results from missing, neglected, or damaged records, protection, and storage of online information content. Currently, information content preservation lacks norms; some platforms improperly manage website content and webpage changes, neglecting identification, storage, and timely updates of online information content, while weakened or outdated recording and preservation technologies also cause memory loss. On the other hand, memory loss results from disappearance of online information platforms and related elements, such as website closures, webpage deletions, link failures, information alterations, information theft, data damage, and data deletion. For example, CSDN knowledge community users' reported loss of published articles and information loss after the elimination of early BBS forums and Renren.com. Additionally, information silos, information islands, and information cocoons cause information memory solidification and isolation, hindering new information inflow and preventing online information memory formation. (2) **Online information content memory dissolution**: On one hand, with various streaming platforms continuously entering online platforms, online hot content faces "replacement dissolution" risks. Before being deeply understood by users and generating meaningful 沉淀, existing online information content is replaced by new hotspots in short periods, presenting a fast-food, assembly-line emergence-dissolution state that hinders good online collective memory formation. On the other hand, information explosion-induced overload affects netizens' memory of online information content, causing memory

fatigue, disorder, rejection, and burden—negative memory dissolution. For example, "tolerance" and "numbness" tendencies toward negative evaluations of positive online events, typified by the "Jiang Ge's mother eating human blood buns" incident, where positive memory effects of online information content are numbed and negatively rejected and dissolved. Additionally, online information pollution content causes memory disorders and distortion, as continuously proliferating online information garbage, harmful and toxic information, and false information affect users' ability to identify information content, hindering formation and storage of authentic and healthy information memory and causing memory disorders and deviations [35]. (3) **Data idleness**: Unused or underutilized data prevents collective memory formation and dissolution. (4) **Online information content memory fragmentation**: As various streaming platforms, social networks, instant messaging apps, and knowledge Q&A communities increasingly enter the internet, alongside specialized, domain-specific, and multimodal search engines, online information memory materials increasingly present fragmented flow storage forms, making complete storage records for collective memory difficult. Users' fragmented information utilization methods also fragment information content memory, threatening complete, orderly, and systematic memory.

---

5. Impacts of Online Information Content Ecosystem Security Risks

Various types of online information content ecosystem security risks constitute the most fundamental and core components of the online information ecosystem security risk system. Security risks generated by online information content directly affect netizen cognition, further influencing netizen behaviors, values, and ideologies during cognitive formation processes. Through individual risk chains, they radiate to the online information ecosystem security space acted upon by online information content units, affecting the basic order, ecological structure, and civilizational degree of the ecological environment required for online information ecosystem security. Based on this, this paper analyzes specific risk type impacts from perspectives of relationships between specific risk types and overall online information ecosystem security risks, interactions among various subjects and specific object factors, and specific roles of typical risk types in online information content ecosystem security risk flows. The analytical framework is shown in Figure 1 [Figure 1: see original paper].

5.1 Mutual Overlap Among Various Risk Type Impacts

From the perspective of relationships between various risks and overall online information ecosystem security risks, different risk impacts overlap. Traditional online information security risks, new online information content security risks, and potential risks from new technology applications intertwine, forming com-

plex and diverse risk chains. Although specific risk data and their variants—such as online ideological risks, online information content vulgarization risks, online information content manipulation risks, online intellectual property risks, and memory disappearance risks—differ in manifestation, they overlap in risk chain impacts. For example, Google's "withdrawal" incident and Apple's "tracking gate" incident reflect international hegemonism's interference in online public opinion and hostile actions against China, showing how some states and actors use cyberspace to manipulate and undermine online ideological security. Deepfake-induced online information content manipulation risks also involve online ideological security issues and affect national digital discourse power in cyberspace. Online content vulgarization risks also weaken mainstream cultural values in cyberspace to some extent, affecting online ideological security. Digital espionage and data tampering in memory disappearance risks also become tools for online information manipulation risks. As variants of various risk types increase, risk chains of interactions among different risk types also multiply. Overlaps among different risk chains create 叠加 effects, resulting in greater threat degrees and scopes than single-dimensional risk impacts, continuously weakening controllability of online information content ecosystem security and posing severe tests and challenges for governance.

5.2 Networked Radiation of Various Risk Type Impacts

From the perspective of interactions among various stakeholders and objects, different risk types expand in scope and degree through networked radiation, continuously reducing stability of the online information content ecosystem security system.

In the online information content ecosystem security risk system, various risk types intertwine with stakeholders including online information content producers, disseminators, service platforms, recipients, and regulators, as well as interest objects represented by online information content itself. Different risk chains converge into a radial diffusion network structure through interactions among different stakeholders and objects, expanding risk impact coverage and degree, thereby intensifying threat and destructiveness of overall online information content security risks. For example, using online ideological threat content objects as intermediaries, online information content service platforms play roles as both disseminators and regulators, while users act as recipients and consumers. When users' awareness of mainstream values is weak and platforms fail to provide effective content screening, trust challenges between users and platforms arise, causing 失调 in online information content subject relationships and affecting stability of the online information content ideological ecology. Similarly, in open environments, influenced by user-centric views and traffic/profit motives, online information content platforms tend to cater to popular lowbrow demands, lowering quality thresholds for information content objects and increasing dissemination of vulgar, intellectual property-infringing, and manipulated content, causing trust challenges between platforms and users and affecting stability of

the online information content ecosystem.

5.3 Continuous Multi-Level Erosion by Various Risk Type Impacts

From the perspective of risk flows in online information content ecosystem security risks, continuous erosion and fission at micro, meso, and macro levels intensify imbalances in the online information content ecosystem security system.

Compared with traditional cybersecurity risks, the high integration and fission characteristics of online information content cause various risks to directly affect all stakeholders and interest objects in the online information content ecosystem security system across three levels: risk prototype fermentation at the micro data variant stage, risk diffusion at the meso risk chain overlap stage, and overall cyberspace destruction at the macro multi-dimensional risk erosion stage. This results in broader harm scopes, more harm objects, and deeper harm degrees. From property, rights, data memory, and cyber cultural environment threats triggered by online information content to superstructure-level online ideological threats, various risks continuously operate and ferment, enhancing the "single trigger affects whole body" destructive power and intensifying system imbalances. For example, under the Web 2.0 environment, UGC has become a fundamental development trend, giving networks enormous social mobilization functions. Once netizens focus on a particular viewpoint or issue, online information content units can generate fission energy, releasing immeasurable risk forces that affect cyberspace ecological security stability. Moreover, open development provides conditions for easy information content access, making information behaviors more uncertain, dynamic, and covert. Illegal actors can anonymously implement data security threats like interception, forgery, and tampering, then hide by diving and erasing traces, switching legitimate identities at will. This phenomenon is particularly evident in catalyzing online content intellectual property risks, information content vulgarization risks, and information content manipulation risks. The randomness and irregularity of online infringement behaviors in cyberspace make them difficult to detect and 取证. Additionally, in open environments, online content data presents diversity, unstructured formats, and non-relevance, often lacking sufficient context, valid associations, and order, increasing obstacles for users' collective memory understanding and meaning construction.

Overall, typical online information content security risks target specific manifestations of different risk types, forming different risks under various factors. These risks continuously erode and ferment at multiple levels, making governance of emerging online information content ecosystem security risks an imminent priority. Facing continuously emerging risks, diversified, persistent, and systematic online information content ecological governance has become an important issue that cannot be ignored. This paper, from an ecological thinking perspective, analyzes the connotation of online information content ecosystem security risks—including specific subject, object, and external environmental

elements—classifies risk types based on relevant laws, policies, and literature, analyzes causes of typical risk content for specific types, and conducts holistic impact analysis from the perspective of relationships between specific risk types and overall online information content ecosystem security risks, aiming to support subsequent extended research on online information content ecosystem security risk types and specific content, and provide foundational basis for constructing systematic online information security risk governance systems.

References

[1] The Logic and Key Points of Xi Jinping's Cyber Power Strategy [EB/OL]. [2021-09-19]. https://m.thepaper.cn/baijiahao_{12203817}.

[2] Cai Qi, Yuan Hui. Research on Network Ecological Security [J]. News Outpost, 2016(8): 34-36.

[3] Cybersecurity Law of the People's Republic of China [EB/OL]. [2021-09-19]. http://www.cac.gov.cn/2018-08/02/c_{1123212094}.htm.

[4] Regulations on the Governance of Online Information Content Ecology [EB/OL]. [2021-09-19]. http://www.cac.gov.cn/2019-12/20/c_{1578375159509309}.htm.

[5] Administrative Measures for Internet Information Services [EB/OL]. [2021-09-19]. http://www.scio.gov.cn/zxbd/zcfg/document/1169111/1169111.htm.

[6] Li Zhenshan. Research on Online Information Content Security Issues [J]. Computer Security, 2011(2): 60-63.

[7] Cui Ling, Ni Hongwei, Gao Yuhui, et al. Overview of WEB Information Content Security Development [J]. Information Security and Communications Privacy, 2019(6): 36-45.

[8] ISO31000 Risk Management [EB/OL]. [2021-09-21]. https://safetyculture.com/checklists/iso-31000-risk-management/.

[9] Tian Li, Liu Ningning, Peng Binghui. Review of Cybersecurity Awareness Research [J]. Information Security and Communications Privacy, 2019(6): 36-45.

[10] He Wei. Online Pushers: Information Manipulation in Network Communication [J]. Internet World, 2011(2): 75-76.

[11] Zhang Taofu. New Media Technology Iteration and Reconstruction of International Discourse Power [J]. People's Tribune · Academic Frontier, 2020(8): 6-11.

[12] Li Yinghui, Anna, Bi Ying. Real Risks and Ideal Governance of National Ideological Security from the Perspective of Network Pseudo-Environment [J]. Qinghai Social Sciences, 2018(6): 63-70.

[13] Zhang Yue. Perspective on the "Stubborn Disease" of New Media Content Vulgarization [J]. People's Tribune, 2019(20): 120-121.

[14] Yang Wenhua, Li Penghao, Li Yunwei. Network Risks and Defense Strategies Facing National Ideology from the Perspective of Security Studies [J]. Theory and Reform, 2015(4): 167-170.

[15] Chen Wei, Zhang Ping, Dai Hua, et al. Control Technologies and Countermeasures for New Cybersecurity Risks [J]. Journal of Nanjing University of Posts and Telecommunications (Social Science Edition), 2021, 23(24): 1-10.

[16] Xu Longbing, Yan Haiming, Zhang Xiaofei. Research Progress on Information-Based Market Manipulation Behaviors [J]. Economic Perspectives, 2018(7): 130-140.

[17] Li Yufeng, Deng Sidi. New Governance Model for Internet Platform Intellectual Property Infringement—Moving Toward Pluralistic Governance [J]. Journal of Chongqing University (Social Science Edition), 2021, 27(2): 155-165.

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

[19] Yu Xiaoyao. Reflection and Ethical Reconstruction on the "Vulgarization" Phenomenon of New Media Content [J]. Chinese Editors Journal, 2018(4): 64-69.

[20] Editorial Department. Implementation Phase of the Regulations on the Governance of Online Information Content Ecology [J]. China Information Security, 2020(2): 54-55.

[21] LIEW C L, OLIVER G, WATKINS M. Insights from Social Media Use by Memory Institutions in New Zealand: Participatory vs Curatorial Culture [J]. Online Information Review, 2018, 42(1): 93-106.

[22] Xu Wendi. Remembering and Forgetting—Research on Social Memory Construction in the Social Media Era [D]. Jinan: Shandong University, 2019.

[23] Zhu Haoqi. Building a Full-Link Content Risk Control System to Solve Content Security Challenges [J]. China Information Security, 2020(2): 73-74.

[24] Xinhua Net. National Cyberspace Administration Launches 2020 "Clear and Bright" Summer Online Environment Special Rectification for Minors [EB/OL]. [2021-09-31]. http://www.gov.cn/xinwen/2020-07/13/content_{5526452}.htm.

[25] Stop Rehabilitating Landlords and Tyrants—Zhou Bapi Exploited Working People, Is He a Good Person? [EB/OL]. [2021-09-21]. https://www.sohu.com/a/420500201_{120797296}.

[26] Stop Demonizing Chinese Dama [EB/OL]. [2021-09-21]. http://hainan.ifeng.com/news/shiping/detail_{{{

[27] Netizens Are Furious! She Actually Said in a Public Speech That China's Air Is Poisonous While America's Air Is Sweet… [EB/OL]. [2021-09-21]. https://www.sohu.com/a/142790001_{469218}.

[28] Shao Peiren. Media Ecology: Media as Green Ecology Research [M]. Beijing: China University of Communication Press, 2008.

[29] People's Daily Public Opinion Monitoring Room. Online Vulgar Language Investigation Report [EB/OL]. [2021-09-31]. http://www.gov.cn/xinwen/2020-07/13/content_{5526452}.htm.

[30] Chen Tiao. Identification of Subjective Intent in Information-Based Market Manipulation [J]. Huabei Finance, 2018(10): 30-38.

[31] Yang Su. Ubiquitous Market Manipulation from the Xu Xiang Case [N]. Securities Times, 2016-12-03(A03).

[32] He Guihua. Research on Problems and Countermeasures in the Online Intellectual Property Protection System [J]. Theory Guide, 2007(9): 71-73.

[33] Online Intellectual Property [EB/OL]. [2021-10-30]. https://baike.so.com/doc/1753557-1854125.html.

[34] Su Lingling. Research on Online Copyright Infringement Manifestations and Protection Regulations in China [J]. Publishing Wide Angle, 2020(14): 40-42.

[35] Ma Linqing. Archives and Collective Memory in the New Media Era [J]. Journal of Information Resources Management, 2014(2): 101-105.

Author Contributions:
Li Jie: Drafted the manuscript;
Zhou Yi: Proposed the research framework and revised the final manuscript.

Publishing Ethics Statement of *Library and Information Service* Magazine

To strengthen and enhance academic norms, research integrity, and academic ethics in paper writing, review, and editing, foster good academic atmosphere, promote scientific spirit, resolutely resist academic misconduct, and establish and maintain a fair, just, and open academic exchange ecological environment, the *Library and Information Service* Magazine (including the editorial departments of *Library and Information Service* and *Knowledge Management Forum*) has formulated this publishing ethics statement, officially released in February 2020.

This publishing ethics statement commits that the two journals will strictly abide by and implement national policies and regulations related to academic ethics and editing and publishing, standardizing the behaviors of authors, peer reviewers, and journal editors throughout the entire editing and publishing process, and accepting supervision from the academic community and society at large. The statement consists of three parts with fifteen clauses: (1) Author

publishing ethics (Academic papers are important components of scientific research; Academic misconduct is a cancer in academic papers; Authors are the main contributors to academic papers; Author signatures reflect intellectual property and academic contributions; Academic papers must attach great importance to intellectual property and information security; Normative citation of references is an important manifestation of academic norms; Great importance must be attached to the normative management of research data; Establish error correction and academic self-purification mechanisms). (2) Peer reviewer publishing ethics (Peer review is an important quality control mechanism for papers; Review experts should comply with relevant ethical guidelines and codes of conduct). (3) Editor publishing ethics (Editors should become guardians of academic paper quality; Editors should play a monitoring role in academic ethics construction; Editors should become the last barrier against academic misconduct; Editors should implement a "zero tolerance" policy toward academic misconduct).

Full text available at: http://www.lis.ac.cn/CN/column/column291.shtml

(Journal News)

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