Research on Infrastructure Development for Intelligence Operations Against Disinformation: Postprint

Authors: Chen Meihua, Wang Yanfei

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

Abstract

[Purpose/Significance] The information fog dilemma in the big data era represents a major challenge confronting national security and development in the new era. How to effectively counter misinformation constitutes one of the crucial research topics for breaking through the information fog. To effectively leverage the role of intelligence in supporting national development strategic decision-making, exploring countermeasures for the foundational construction of intelligence work against misinformation by integrating practical experience and theoretical methods serves as an effective breakthrough point for enhancing intelligence system capabilities. [Method/Process] Departing from the broad context of the current "infodemic," this study clarifies the fundamental understanding of misinformation within the information fog dilemma. Based on a summary of existing research and case analysis of misinformation countermeasures in the United States and the European Union, the ecological concept is introduced to construct an intelligence work model for addressing misinformation. Finally, from the perspectives of information ecology subject elements and information ecology environmental elements, countermeasures for the foundational construction of intelligence work against misinformation are proposed. [Results/Conclusion] The foundational construction of intelligence work to counter misinformation requires strengthening collaboration among information governance actors; enhancing the level of intelligence personnel training and public intelligence literacy through a parallel approach of specialized intelligence education and general education; optimizing information governance institutions, developing professional technical tools, improving management and evaluation mechanisms, and consolidating the intelligence foundation for effectively countering misinformation.

Full Text

Abstract

[**Purpose/Significance**] The dilemma of information fog in the era of big data represents a major challenge to national security and development in the new era, and how to effectively address disinformation constitutes one of the critical research topics for breaking through information fog. To fully leverage intelligence support for national development strategic decision-making, exploring countermeasures for intelligence infrastructure construction against disinformation by combining practical experience with theoretical methods offers an effective breakthrough point for enhancing intelligence system capabilities. [**Method/Process**] Beginning with the current backdrop of the "information epidemic," this paper clarifies fundamental understandings of disinformation within the information fog dilemma. Based on a review of existing research and case analyses of U.S. and EU responses to disinformation, it introduces ecological concepts to construct an intelligence work model for addressing disinformation. Finally, from the perspectives of information ecology subject elements and information ecology environmental elements, it proposes infrastructure construction countermeasures for intelligence work to counter disinformation. [**Result/Conclusion**] Infrastructure construction for intelligence work against disinformation requires strengthening collaboration among information governance entities; improving intelligence talent cultivation and public information literacy through parallel specialized and universal intelligence education; optimizing information governance systems; developing professional technical tools; and improving management and evaluation mechanisms to establish a solid intelligence foundation for effectively addressing disinformation.

Keywords: disinformation; intelligence work; information epidemic; information ecology

Classification Number: G250

DOI: 10.13266/j.issn.0252-3116.2021.21.012

1. Introduction

With the rapid development of information processing and transmission technologies, big data has become the defining characteristic of the information society. However, as information volume continues to grow, we face increasingly numerous information-related problems. L. Rosenberger notes that if one word could define our contemporary information environment, it would be "disorientation" [1]. In 2016, the Oxford Dictionary selected "post-truth" as its Word of the Year. In 2017, "fake news" was chosen by the Collins English Dictionary as its Word of the Year. In 2018, researchers J. Kavanagh and M. D. Rich from the RAND Corporation published a lengthy report on "truth decay," arguing that due to the spread of disinformation, the role of facts, data, and analysis in political and civic discourse and decision-making processes is grad-

ually diminishing [2]. "Truth decay" has become a specialized term proposed by RAND Corporation based on the development of the information era, with multiple research projects launched around this concept. In 2019, *Nature* published an article titled "The Spread of Disinformation: Bots, Trolls, and All of Us," pointing out that disinformation attacks the most vulnerable part of our value system—its core, namely social values; misunderstanding disinformation makes us more susceptible to online manipulation [3]. During the global COVID-19 pandemic outbreak in 2020, the spread of disinformation severely impacted epidemic prevention and information governance processes, drawing increasing attention from think tanks and scholars. As K. Hao et al. noted in *MIT Technology Review*, the coronavirus triggered the first true "infodemic" of modern social media [4].

In this context, intelligence work faces major transformation. On one hand, open-source information provides richer intelligence sources and is increasingly becoming an important research content, bringing new opportunities for the transformation and development of intelligence work. On the other hand, facing the real information fog dilemma of the post-truth era, fake news, and truth decay in the big data era, traditional intelligence infrastructure and service mechanisms centered on information resource organization and information technology iteration cannot meet the comprehensive and specialized intelligence needs of China's innovation-driven development strategy. Many scholars have begun to re-examine the focus of intelligence work and theoretical research in China, proposing to shift intelligence work priorities to mission-context-oriented strategic foresight and rapid response. This requires greater emphasis in intelligence infrastructure construction on solving information incompleteness problems and attaching more importance to guarantee conditions for achieving intelligence work objectives.

2. Cognitive Analysis of Disinformation

2.1. Clarification of Disinformation Terminology

Current research on disinformation lacks clear conceptual distinctions and unified usage rules, with phenomena of conceptual mixing. The author has surveyed English expressions related to false/incorrect information in existing literature, mainly including *fake information*, *disinformation*, *false information*, and *misinformation*. To ensure accurate conceptual definition and operability and minimize ambiguity, this paper distinguishes several English terms expressing "false" information meanings based on Oxford English Dictionary definitions from an English translation perspective, as follows:

(1) **Fake information** typically refers to fabricated, forged, or elaborately produced news or other types of textual content that is incorrect or nonexistent, usually with the purpose of misleading or deceiving. In the late 19th and early 20th centuries, the practice of "faking" news stories sparked widespread discussion in American newspaper journalism. Currently, it

mainly exists in two forms: first, spreading inaccurate content through social media or the internet, especially content with specific political or ideological purposes; second, attempting to discredit or portray media reports as partisan or untrustworthy.

(2) **Disinformation** refers to deliberately spread false information, especially that provided by governments or their agencies to foreign governments or media, emphasizing the erroneous nature of information, including incorrectly associated and misleading information. The term originated from the Russian *dezinformacija* coined in 1949. Given the Soviet Union's political and cultural environment at the time, the connection between disinformation and negative, malicious content may have been a product of Stalinist information control policy development.

(3) **False information** mainly refers to content expressing untruthful information, while *false* in the military field also refers to deceptive information with the purpose of deception.

(4) **Misinformation** has two meanings: first, the act of misleading others or the state of being misled; second, incorrect or misleading information. According to the Oxford English Dictionary, the expressions of several disinformation terms have subtle differences. *False information* and *misinformation* focus more on the erroneous nature of information, while *fake information* has greater similarity with *disinformation*, both emphasizing the erroneous, misleading, and deceptive nature of information with strong purposefulness.

Additionally, there are differences regarding the operational subjects of disinformation. For example, *fake information* appears more frequently in the journalism industry, *disinformation* more often in governments and related institutions or media, while *misinformation* and *false information* appear more in daily communication, social media, and the internet.

2.2. Distinctions by International Organizations and Scholars

2.2.1. UNESCO In 2018, UNESCO compiled the *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*, in which the chapter "Thinking about 'Information Disorder' " distinguishes misinformation, disinformation, and malinformation (see Figure 1 [Figure 1: see original paper]). UNESCO notes that most discussions about "fake news" conflate *misinformation* and *disinformation*. However, misinformation mainly refers to the distribution of verifiably false content that is not intended to cause harm. It also points out from the perspective of freedom of expression that individuals or other actors have the right to express unverifiable or incorrect viewpoints, but digital platforms responsible for spreading misinformation can stop its dissemination according to terms of service. The EU defines *disinformation* as "false content that is created, presented, and disseminated for economic gain or to intentionally deceive the public and may cause public harm" [6]. Malin-

formation primarily aims to "damage, harm," mainly referring to information that causes harm to individuals, organizations, or countries, typically represented by leaked private information, harassing information, and hate speech. Disinformation falls between the two, mainly involving information produced in wrong contexts, impersonated information, and deliberately fabricated information. Disseminators usually know it is false, so disinformation has both the erroneous attribute of misinformation and the purposeful intent to damage of malinformation. Furthermore, UNESCO believes these three types of disinformation may appear in combination as part of specific information strategies, meaning individual disinformation types usually accompany other information types. However, clearly distinguishing these three types will help clarify the causes of such information and actively adopt corresponding remedial measures [5].

2.2.2. European Union The EU has specifically made basic terminological distinctions between *misinformation* and *disinformation*, defining *misinformation* as the distribution of false content that is verifiable and not intended to cause harm, while also noting from the freedom of expression perspective that individuals or other actors have the right to express unverifiable or incorrect viewpoints. Digital platforms can stop the spread of misinformation according to service terms. The EU defines *disinformation* as "false content that is created, presented, and disseminated for economic gain or to intentionally deceive the public and may cause public harm" [6].

2.2.3. Scholarly Distinctions on Disinformation Early scholars often viewed *disinformation* as a type of *misinformation* [7-8]. However, D. Fallis argues that disinformation includes three characteristics: disinformation is a kind of information; disinformation is misleading; and disinformation is non-accidental. He believes disinformation is usually inaccurate but not necessarily so—it only must be misleading. Therefore, disinformation is not actually a subset of misinformation [9]. N. A. Karlova et al. further listed the characteristics of information, misinformation, and disinformation in a table, proving that misinformation and disinformation are distinctly different but equal subcategories of information [10]. J. Pamment from the Carnegie Endowment for International Peace, who specializes in disinformation research, proposed in a series of reports on EU disinformation that a new, more precise terminology for disinformation needs to be developed. He argues that the term "disinformation" is used as a blanket term covering all influence activities, while current EU policies on disinformation cannot fully suit the purpose of countering disinformation, thus requiring new terminology to add nuance and precision to EU policies [11].

Based on the above analysis, some early evidence regarding disinformation terminology may not represent fixed collocations. As K. Starbird noted in the *Nature* article, disinformation cannot be distinguished merely through "true" and "false" labels; it often involves accurate facts presented in misleading contexts. Meanwhile, disinformation originates not only from automated accounts

(bots) or internet trolls that generate false content but also requires a variety of participants for effective disinformation campaigns, possibly including mostly unwitting actors [3]. The author is more inclined to view these as terms that have received varying degrees of attention during different periods of information society development, each with its own focus but also with blurred boundaries that can transform under certain contextual conditions. This paper primarily analyzes disinformation (*disinformation*) that emphasizes misleading functional characteristics.

3. Related Research and Case Analysis on Dealing with Disinformation

3.1. Related Research on Dealing with Disinformation

In recent years, disinformation has attracted attention from experts in communication studies, computer science, information science, psychology, and many other disciplines. This paper surveyed literature on addressing disinformation through CNKI, Web of Science, ProQuest, and other databases, and summarized research content on disinformation in related fields.

3.1.1. Communication Studies Research Research in this field mainly focuses on disinformation governance on social media. K. Shu et al. introduced types and distinctions of information disorder on social media and proposed a weakly supervised method to detect disinformation with limited labeled data [12]. A. K. Natascha and E. F. Karen established a social diffusion model of misinformation and disinformation from an information behavior perspective, arguing that people's judgment of disinformation is closely related to information literacy [13]. V. L. Rubin viewed misinformation and disinformation as a sociocultural-technology-driven epidemic in digital news disseminated through social media, and based on the epidemiological triangle model, proposed a conceptual model for misinformation and disinformation, suggesting three intervention measures—automation, education, and regulation—to prevent disinformation spread [14].

3.1.2. Computer Science Research Research in this field mainly focuses on exploring technical methods for disinformation detection and filtering. Wang Yonggang et al. proposed a social network disinformation propagation control method, Fidic, which narrows the spread of disinformation by rating users and controlling the propagation behavior of high-rated users, ultimately achieving the goal of curbing or even eliminating disinformation spread [15]. Wu Ye et al. systematically reviewed the advancement of computational methods in disinformation propagation research from three perspectives—disinformation content characteristics, disseminator user characteristics, and disinformation propagation patterns—and discussed future feasible interdisciplinary cooperation models [16]. S. T. Smith et al. proposed an end-to-end framework to automatically detect disinformation and influential network participants, verifying the

effectiveness of the monitoring system by collecting Twitter datasets during the 2017 French presidential election to identify high-influence accounts [17]. Huang Wenhua and Wang Lei et al. successively proposed filtering methods based on received signal strength, achieving efficient disinformation filtering according to the relationship between sensor-received signal strength and propagation path attenuation index [18-19].

3.1.3. Information Science Research Research in this field mainly focuses on enhancing public ability to deal with disinformation through library information literacy education and media information literacy education. Y. Hwang et al. investigated the negative impact of disinformation including deepfake videos and the protective role of media literacy, and through three media literacy factor designs using two types of disinformation experiments, demonstrated that disinformation including deepfake videos is more vivid, persuasive, credible, and likely to be shared, while media literacy education will reduce the impact of disinformation [20]. Zhou Yaqi et al. argued that during the COVID-19 pandemic, disinformation was rampant, and libraries should treat disinformation governance as an important part of emergency services, proposing basic ideas for library participation in disinformation governance through investigation [21]. Jiang Jinyan studied cases of U.S. library participation in combating online disinformation, providing certain experience for domestic libraries [22]. Huang Yuting and Wang Jingxia respectively explored paths to improve public disinformation discrimination ability from the perspectives of information literacy and public media information literacy, providing countermeasures for increasingly severe disinformation [23-24].

3.1.4. Research in Other Related Fields In 2009, D. Fallis discussed the concept of disinformation using philosophical methods of conceptual analysis in "A Conceptual Analysis of Disinformation," briefly discussing how this analysis could help us deal with disinformation problems [9]. In 2015, in "What is Disinformation," he summarized and analyzed various viewpoints on information proposed by renowned information scientists and philosophers, pointed out the limitations of existing conceptual analysis scope for *disinformation*, and argued that *disinformation* is misleading information with misleading functions, briefly discussing how this analysis could help develop technologies for detecting disinformation and policies for stopping its spread [25].

In social psychology, C. Wolverton and D. Stevens, based on the Five-Factor Model (FFM) of personality traits, investigated and quantified the impact of personality traits on disinformation identification ability through snowball sampling. The research results enable companies to identify customers, investors, and other stakeholders most likely to be deceived by disinformation, better preparing for and responding to organizational impacts of disinformation [26].

3.2. Case Analysis of Dealing with Disinformation

Disinformation with misleading characteristics has features of wide propagation range, fast propagation speed, and diversified propagation media in the internet environment. Therefore, it is both an important means of information warfare used by some Western countries externally and an extension of their domestic political tools. Based on the fact that terms like "disinformation" and "disinformation campaigns" are widely mentioned and utilized in Western political circles, this paper selects practical cases of the U.S. government, think tank organizations, and the EU as a regional organization in dealing with disinformation for analysis. This can effectively grasp the basic thinking of Western countries regarding disinformation and provide insights for China's intelligence infrastructure construction in response to disinformation.

3.2.1. United States (1) Relevant U.S. Government Measures and Acts

- **Establishment of the Cognitive Security Intelligence Center (CSIC) – Building a Support Platform and Enhancing Technical Support.** The 2020 U.S. National Defense Authorization Act (NDAA) required the establishment of a social media data and threat analysis center to address the growing threat of disinformation, namely the Cognitive Security Intelligence Center (CSIC) [27]. In fact, since the 2016 U.S. election, increasing amounts of false and misleading discourse have greatly weakened public trust in democratic institutions. Although some scholars believe CSIC needs more support to realize its full potential in dealing with disinformation and have pointed out existing problems—such as the lack of consistency and coordination in content review strategies across various social media platforms to address the growing threat of disinformation, and the lack of sufficiently advanced and effective anti-disinformation technology [28]—overall, the establishment of CSIC provides a good platform and technical support for dealing with disinformation and represents a major step forward for the government.
- **COVID-19 Disinformation Task Force Act – Optimizing Institutional Framework and Popularizing Information Literacy Education.** On August 6, 2020, the 116th U.S. Senate passed the COVID-19 Misinformation and Disinformation Task Force Act of 2020 [29]. According to the act, an inter-agency COVID-19 (i.e., coronavirus 2019) misinformation and disinformation task force will be established, with members regularly engaging with racial or ethnic minority communities, rural areas, and other underserved populations. The task force's responsibilities include: coordinating analysis of COVID-19 disinformation and misinformation across federal government agencies while protecting privacy and civil liberties; conducting comprehensive analysis of COVID-19 misinformation and disinformation and coordinating reports to federal government agencies and the White House pandemic task force; and conducting and disseminating

pandemic-related information literacy education to raise public awareness. The passage of the task force act and the establishment of the task force will provide a realistic basis for federal government governance of disinformation, while public information literacy education will greatly enhance the public's ability to identify disinformation, effectively reducing its impact.

(2) Research Projects and Related Products of Well-Known U.S. Think Tanks

- **RAND Corporation – Conducting Targeted Research Projects and Using AI to Assist in Developing Response Tools [30].** The emergence of the internet and social media has fundamentally changed the information ecosystem, making it easier for the public to access more information directly while also increasing the difficulty of distinguishing effective information from low-quality or false information. This means the spread of misleading disinformation aimed at achieving economic or political purposes will be even faster. Accordingly, RAND researchers have developed an online database providing information on currently available or developing online tools for identifying disinformation in networks, particularly social media, to address today's challenging information environment. This database is part of RAND's "Truth Decay" project. It mainly includes seven categories: bot/spam detection, codes and standards, disinformation tracking, credibility scoring, education/training, verification, and whitelisting. Its primary purpose is to help users understand the media ecosystem and improve their media literacy. These online tools have achieved a transformation from human fact-checker-supported websites to applications using artificial intelligence for detection, greatly expanding the scope of anti-disinformation tools and providing a roadmap for further development of related projects and tools.

- **Atlantic Council – Emphasizing Participation of Professional Talent and Focusing on Integration of Products and Practice [31].** The Atlantic Council's Digital Forensic Research Lab (DFRLab) was specifically established to address issues such as public dialogue confusion and political polarization that disinformation may cause. The lab comprises multiple disinformation research experts aiming to track, identify, and expose disinformation and fake news through open-source information. Its work sits at the unique intersection of government, media, and technology, ensuring democracy and restoring trust in public discourse by establishing online accountability and transparency, thereby ensuring the scientific validity and effectiveness of disinformation response work to a certain extent. Currently, DFRLab mainly conducts two related projects: (1) Establishing an interactive open-source database—the Foreign Interference Attribution Tracker (FIAT), which captures allegations of foreign interference related to the 2020 election and evaluates each content's credibility, bias, evidence, transparency, and impact; (2) Preparing an election

official handbook for disinformation on election day, which is part of the "Election Integrity Partnership Project." It collects major development trends and investigation results of election-related disinformation in 2020 and provides corresponding recommendations to U.S. election officials, demonstrating effects closely integrated with actual national work.

- **Carnegie Endowment for International Peace – Producing Countermeasure Research Reports and Emphasizing Close Integration with Intelligence Work [32].** On October 21, 2020, the Carnegie Endowment for International Peace published the working group report "The New Weapon of Choice: Technology and Information Operations Today," pointing out that social media and the internet have become primary tools for spreading harmful information. To date, responses from the technology sector and civil society have been insufficient to address current information problems. The report's recommendations section points out that governments need to make internal and external coordination more systematic, and where permissible, must cooperate more closely with relevant countries in intelligence work; regular briefings from the intelligence community or other depoliticized entities can provide real-time updates to media and the public on disinformation campaigns; governments should take more measures to incentivize and strengthen research on information operations, such as establishing rapid response mechanisms. Additionally, the report proposes a series of recommended measures in government supervision, domain norms, and education and publicity, providing an important basis for governments to take further countermeasures.

3.2.2. European Union (1) Code of Practice on Disinformation – Reaching Consensus on Behavioral Norms for Mainstream Online Platforms and Forming Effective Supervision Mechanisms [33].

To address the spread of online disinformation and fake news, on September 26, 2018, under EU organization, some online platforms, mainstream social networks, advertisers, and advertising industry representatives unanimously reached a self-regulatory code of practice, namely the *Code of Practice on Disinformation*. The code aims to achieve the EU Commission's goals proposed in April 2018, ranging from transparency in political advertising to closing fake accounts and demonetizing disinformation providers. The code also includes an annex identifying best practices that signatories will use to implement it. In October 2018, online platforms Facebook, Google, Twitter, Mozilla, and some advertisers and advertising industry representatives signed the code and introduced their respective roadmaps for implementation. Signatories regularly submit baseline reports to the EU, which also conducts targeted monitoring of their implementation. The EU Commission released the signatories' annual self-assessment report for the Code of Practice in 2019 and an assessment report in September 2020, while pointing out problems in the implementation process. Subsequently, Microsoft and TikTok signed the agreement in May 2019 and

June 2020, respectively. The Code of Practice on Disinformation represents the first global consensus among industry sectors to combat disinformation through self-regulatory codes and is an important means of forming effective supervision mechanisms for mainstream online platforms.

(2) Action Plan Against Disinformation – Real-Time Monitoring, Cross-Departmental and Cross-Organizational Collaboration to Achieve Intelligence Analysis, Assessment, and Sharing [34].

The Action Plan Against Disinformation aims to strengthen cooperation between member states and the EU in four key areas: improving monitoring; coordinating response measures; cooperating with online platforms and industry; and raising citizen awareness and enhancing citizens' ability to respond to online disinformation. Currently, information platform construction responding to the Action Plan mainly includes the Rapid Alert System (RAS) and the European Digital Media Observatory (EDMO). RAS, as a dedicated digital platform, is a network composed of 28 national contact points and a convergence point for academia, fact-checkers, online platforms, and international partners. It is an important component of the EU's overall approach to disinformation, allowing EU member states and institutions to share disinformation activity instances and discuss best response measures through this platform. EDMO mainly serves as a hub for fact-checkers, academics, and other stakeholders to collaborate, aiming to deepen understanding of the disinformation phenomenon while providing support for media organizations, media literacy experts, and decision-makers. Additionally, EDMO will initially focus on deploying core service infrastructure and defining the observatory's governance rules; later, it will establish EDMO national or regional digital media research centers across EU territory. The Action Plan's information platform conducts real-time monitoring through technical support and is committed to cross-organizational and cross-departmental collaboration, laying a realistic foundation for intelligence work to achieve analysis, assessment, and sharing in response to disinformation.

4. Ecological Perspective on Intelligence Work for Dealing with Disinformation

Based on fundamental understandings of disinformation and case analyses of U.S. and EU responses, the author believes that from an intelligence studies perspective, addressing disinformation is important work for effectively solving various risks and uncertainties in decision-making within information fog. This section uses ecological concepts to explore an ecological model of intelligence work for dealing with disinformation, striving to achieve a symbiotic, coexistent, and progressive information governance ecosystem through improved intelligence infrastructure construction.

4.1. The Role of Ecological Concepts in Intelligence Work Against Disinformation

4.1.1. Intelligence Work Against Disinformation as a Guarantee for Maintaining Information Ecosystem Balance and Healthy Development The current information technology revolution has greatly lowered the threshold and cost for spreading incorrect information and disinformation, with social media and the internet becoming primary tools for more governments and related institutions, organizations, and personnel to spread disinformation against opponents. Particularly with the global outbreak of COVID-19, these activities have intensified, and the information ecosystem faces severe challenges. Therefore, information filtering, threat analysis, and intelligence assessment have become important components of disinformation response work.

The mission of intelligence work is to solve information incompleteness problems in decision-making processes, with its main value lying in foreseeing new problems and identifying new symptoms to support decision-makers in making early strategic arrangements when information is incomplete. From a cognitive perspective, people's grasp of information has four states: known-known, known-unknown, unknown-known, and unknown-unknown [35]. Intelligence work for healthy information ecosystem development is achieved through intelligence perception, intelligence characterization, and intelligence response capabilities supported by various intelligence infrastructure conditions, enabling information collection, processing, and analysis to form cognition, interpretation, and expression of intelligence user needs, intelligence object content, and intelligence tasks, with intelligence products as the main form to support strategic decision-making [36]. The process of intelligence infrastructure supporting intelligence work itself is a response to information ecosystem imbalance and constitutes important intelligence infrastructure conditions for dealing with disinformation.

4.1.2. Information Ecology Concepts as the Foundation for Intelligence Work Against Disinformation China's national comprehensive security and development information environment is undergoing rapid change, and intelligence agencies' ability to predict and respond to changes faces severe tests. Big data and noise data from networks, physical sensors, and various other information environment media continue to increase, while signals with intelligence identification value are weak, dispersed, and difficult to manifest [37]. Intelligence work during social transformation often risks being reactive rather than strategic, lacking corresponding integrated management references in intelligence enterprise management, with ad hoc incident handling becoming the norm for intelligence management work related to the information society. Therefore, focusing on dynamic development, exploring cross-boundary and cross-domain analysis, and organizing information ecology governance under new circumstances has become particularly urgent [38].

The research object of information ecology is the information ecosystem, which achieves healthy information ecosystem development by analyzing and studying

relationships among various ecological factors within the information ecosystem [39]. Chinese and foreign scholars have found in research and analysis on intelligence failure that "uncertainty is the fundamental attribute of intelligence. Only through unremitting efforts can intelligence agencies obtain knowledge about adversaries" [40]. It is precisely because of these continuous efforts to adjust systems and processes in response to environmental changes that the intelligence ecology can exist and develop healthily. Ecological concepts are the inevitable choice for interpreting complex giant systems such as the information environment. Therefore, the intelligence perspective interpretation of addressing disinformation must emphasize research on intelligence work from an ecological perspective. The key point of the ecological concept interpretation for dealing with disinformation is to view intelligence work as an ecosystem composed of elements such as intelligence agencies, intelligence personnel, intelligence education, and intelligence systems, with self-organizing, self-growing, and self-correcting functions [35].

4.2. Construction of an Intelligence Work Model for Dealing with Disinformation

According to basic information ecology theory, information, information people, and information environment jointly constitute the element set of the information ecosystem [41]. In the process of disinformation governance, intelligence system capabilities in intelligence perception, intelligence characterization, and intelligence response also cannot be separated from the construction and coordination of various elements of the information ecosystem, as shown in Figure 2 [Figure 2: see original paper].

4.2.1. Intelligence Perception of Multi-Source Heterogeneous Information In the big data era, the fundamental change intelligence work faces first is the change in intelligence sources, mainly reflected in changes in information volume, information structure, and information quality. In the big data era, people seem to generally focus more on actively utilizing information processing and transmission technologies, while problems such as "information pollution," "information overload," "information redundancy," and "information fog" caused by massive amounts of information are easily overlooked.

4.2.2. Intelligence Characterization Oriented Toward Information People Intelligence characterization refers to the process where intelligence analysts construct intelligence products or services that enable clients to quickly perceive after identifying information [42]. According to information ecology theory, all participants in a series of disinformation activities in a disinformation environment can be called information people. The main information people factors in disinformation involve governments and related institutions, media, and the public. As information subjects in the information ecosystem, they have clear role boundaries while also being interdependent and transformative,

possibly playing different roles at different stages and occasions. Various subject factors continuously adjust and co-evolve in the information environment. Intelligence characterization oriented toward information people will carefully and accurately extract attributes of intelligence-related matters, prioritize facts, and make content and external characteristics of intelligence easier to perceive accurately and quickly, which is key to more effectively responding to disinformation.

4.2.3. Intelligence Response in the Information Environment The information environment is the sum of all information elements surrounding humans and social organizations in the information ecosystem. In disinformation governance, factors such as information technology, information laws and policies or ethics, and information quality education are effective guarantees for intelligence infrastructure to respond to intelligence system capabilities and enhance disinformation governance effectiveness. The improvement of these environmental factors mainly plays guiding, promoting, standardizing, and restraining roles, which will help create a healthy information ecology. With the rapid development of information technology and increasing demands of the information society, the information market has developed rapidly, but a series of contradictions have emerged in political, economic, cultural, and other fields. Therefore, we must recognize the importance of information infrastructure environmental factor response to disinformation governance.

These three aspects are independent yet have closely interdependent and mutually influential relationships: multi-source heterogeneous information for intelligence perception mainly comes from information exchange and dissemination by information people in different forms, while information acquisition, processing, and processing are also influenced by intelligence technology; information environmental factors such as education, systems, and ethics directly or indirectly influence information people's information behavior or information literacy; and the effectiveness of intelligence characterization oriented toward information people also depends on intelligence perception capabilities and information environmental factors such as intelligence technology and systems. Clarifying the information ecosystem formed by these information factors is an effective entry point for exploring intelligence work response to disinformation governance.

5. Countermeasures for Intelligence Infrastructure Construction Against Disinformation

How to effectively address disinformation is a huge challenge and a comprehensive, systematic task. Based on the ecological mechanism analysis of intelligence work against disinformation governance, the work links of intelligence perception, intelligence characterization, and intelligence response in disinformation governance need to be carried out comprehensively and at multiple levels. The author proposes countermeasures for intelligence infrastructure construc-

tion against disinformation from the perspectives of information ecology subjects and information ecology environment, combined with the previous case analysis and intelligence work model construction.

5.1. Cultivation of Information Ecology Subjects

5.1.1. Strengthening Collaboration Among Subjects Dealing with Disinformation On one hand, this involves optimizing the operational models of intelligence organizations. Based on current interdisciplinary integration development trends, inter-organizational jointness and collaboration have increasingly become effective organizational models for intelligence work. In the process of intelligence work against disinformation, breaking organizational boundaries and promoting inter-organizational jointness and collaboration can not only effectively solve problems of insufficient human resources and knowledge reserves in intelligence subject organizations but also greatly enhance the business capabilities and levels of intelligence work for rapid disinformation response. To achieve this goal, it is necessary to consider flat, virtual, and networked work models for cross-departmental and cross-organizational team collaboration within the intelligence system, establishing an integrated intelligence business fusion and collaboration model that integrates relevant intelligence agencies, information management and service institutions, supervision platforms, related professional research resources, and intelligence theories into a whole, promoting the formation of a highly collaborative intelligence work system.

On the other hand, it involves promoting data integration and sharing among various information subjects to achieve rapid disinformation warning through information flow advantages. Establishing data integration and sharing platforms is an effective way to strengthen the integration of existing resources of various information subjects such as government agencies and online media, and also an effective channel for tracking and identifying disinformation. Furthermore, optimizing platform information sharing mechanisms and standardizing information release rules can improve information organizations' ability to quickly obtain effective information from massive amounts of information, forming advantages in information collection, rapid processing, and timely and accurate information release, and timely responding to disinformation governance decision-making [43].

5.1.2. Building Parallel Education Systems for Professional and Vocational Intelligence Talent Disinformation governance needs to rely on a professional talent foundation to ensure the effectiveness and scientific nature of governance work. The demand for disinformation governance talent is not a direct product of intelligence education but emerges from practice in dealing with disinformation. Therefore, constructing and optimizing the intelligence education system is an indispensable intelligence infrastructure condition for providing sufficient professional talent for disinformation governance work. In

response to the current disinformation governance dilemma, China's future intelligence talent cultivation system construction can consider two aspects: (1) Build a specialized intelligence education system. Further clarify the training objectives for intelligence talent, clearly position intelligence research education to meet intelligence business and intelligence enterprise development requirements, enrich intelligence education curriculum content, cultivate intelligence talent with intelligence thinking and skills, and provide professional knowledge and skills for disinformation governance work. (2) Strengthen universal intelligence education. Mainly conducted through regular training and publicity, such as offering intelligence courses for special occupational groups, improving the overall intelligence literacy of the public and professional personnel through online teaching, institutional or project cooperation, pre-job training in specific agencies, and professional qualification training in specific fields, to effectively respond to disinformation governance work.

5.2. Preparation of Information Ecology Environment

5.2.1. System Optimization The Fourth Plenary Session of the 19th CPC Central Committee passed the "Decision of the CPC Central Committee on Upholding and Improving the System of Socialism with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Capacity," which systematically outlined the "map" of the system of socialism with Chinese characteristics for the first time. In the process of deeply understanding the milestone significance of the Fourth Plenary Session and effectively implementing its spirit, it is necessary to uphold the advantages of the system of socialism with Chinese characteristics, comprehensively promote the modernization of the information governance system and intelligence governance capacity in response to national information governance needs and combined with national information governance security work practice [44].

According to the previous case analysis, both the U.S. government and the EU have formulated a series of acts and codes of practice targeting disinformation, but they have not yet shown systematization. China's current information governance adopts a combination of distributed and centralized governance models, initially forming a governance mechanism for cyberspace society. Promoting system construction against disinformation under new circumstances is an important infrastructure condition for the smooth progress of intelligence work, which must be further developed in accordance with the system of socialism with Chinese characteristics. On one hand, strengthen government offensive efforts. Enhance disinformation governance system construction, formulate countermeasures and laws and regulations tailored to disinformation that fit the characteristics of the system of socialism with Chinese characteristics. Disinformation governance involves multi-domain policy formulation and should specifically formulate targeted countermeasures for disinformation to change its strategic evolution in a coordinated manner and prevent the behavior of relevant disinformation leaders. On the other hand, utilize national public opinion supervision

means to promote self-regulation mechanism construction of online media platforms. Under the premise of responding to information governance objectives and tasks, support government agencies and public organizations in monitoring online platform information norm formulation and practice to timely and effectively limit the adverse effects of disinformation dissemination.

5.2.2. Application of Technical Tools and Means The proliferation of disinformation fully demonstrates that current information technology capabilities in monitoring, identifying, analyzing, and sharing information need further improvement. In the big data environment, disinformation driven by information technology reasons must ultimately be solved through technical tools and means. Only by keeping pace with the times and being good at utilizing information technology and specialized technical tools in the intelligence field can we build a first-class intelligence capability system to enhance disinformation governance levels.

Intelligence technology is distributed in all stages of intelligence activities. It is a collection of tools, systems, and techniques used to convert data or information from different sources and structures into valuable intelligence and ultimately achieve intelligence service objectives [45]. The technical application in intelligence response to disinformation will also revolve around the capability application links of intelligence perception, intelligence characterization, and intelligence response. Based on the propagation patterns and stage characteristics of disinformation, using intelligent algorithms, blockchain, and other technologies for dynamic monitoring, noise reduction, identification, filtering, and other technical processing of disinformation is an important means to prevent disinformation diffusion and propagation, reduce the harm degree of disinformation, and maintain the information ecology [46].

5.2.3. Improving Management and Evaluation Mechanisms for Basic Intelligence Response Capabilities Using intelligence infrastructure construction to prepare for intelligence mission response is an important link for the sustainable development of the intelligence enterprise. The objective of disinformation governance intelligence work is to start from national security and development, enhance intelligence system capabilities in monitoring, assessment, and foresight from the perspective of intelligence infrastructure construction, and perceive and identify risks that disinformation poses to national society, economy, and politics. Therefore, establishing and improving evaluation mechanisms for basic intelligence response capabilities is an important means to measure the maturity of intelligence system capability development and an important basis for intelligence infrastructure to respond to information ecosystem balance development.

In the future, it is necessary to determine an evaluation system for intelligence infrastructure construction based on the basic understanding that intelligence infrastructure construction supports intelligence system capabilities, to ensure

the scientificity and effectiveness of intelligence infrastructure management and evaluation.

Conclusion

As a complex giant system, intelligence infrastructure construction is an important guarantee for enhancing intelligence system capabilities to address disinformation and a significant research topic for achieving sustainable intelligence enterprise development. The innovation of this paper lies in integrating existing research, practical cases, and theoretical exploration to explore the important significance of intelligence infrastructure construction in the information fog environment, and introducing ecological concepts into the construction of an intelligence work model for dealing with disinformation based on case analysis to ensure the systematicness and effectiveness of intelligence infrastructure analysis. However, future research must also note that infrastructure construction must form perfect alignment with intelligence work against disinformation and requires gradual progress; the construction of the national overall intelligence system capability needs further optimization and strengthening, and the level and effectiveness of intelligence infrastructure construction for dealing with disinformation also require further demonstration and experimentation. How to address disinformation will remain one of the important challenges facing current and future intelligence work, worthy of in-depth research by academia.

References

[1] ROSENBERGER L. Disinformation disorientation [J]. Journal of democracy, 2020, 31(1): 203-207.

[2] KAVANAGH J, RICH M D. Truth decay: an initial exploration of the diminishing role of facts and analysis in American public life [EB/OL]. [2020-12-10]. https://www.rand.org/pubs/research_{reports}/RR2314.html.

[3] STARBIRD K. Disinformation's spread: bots, trolls and all of us [J]. Nature, 2019, 571(7766): 449.

[4] HAO K, BASU T. The coronavirus is the first true social-media "infodemic" [EB/OL]. [2020-08-21]. https://www.technologyreview.com/2020/02/12/844851/the-coronavirus-is-the-first-true-social-media-infodemic/.

[5] WARDLE C, DERAKHSHAN H. Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. Journalism, 'fake news' & disinformation: handbook for journalism education and training [EB/OL]. [2020-12-09]. https://en.unesco.org/sites/default/files/journalism_{{{fake}}{{news}}}{{{disinform

[6] EUROPEAN COMMISSION. Action plan against disinformation [EB/OL]. [2020-12-11]. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_{en}.pdf.

[7] LOSEE R M. A discipline independent definition of information [J]. Journal of the American Society for Information Science, 1998, 48(3): 254-269.

[8] ZHOU L, BURGOON J, NUNAMAKER J, et al. Automated linguistics based cues for detecting deception in text-based asynchronous computer-mediated communication: an empirical investigation [J]. Group decision negotiation, 2004, 13(1): 81-106.

[9] FALLIS D. A conceptual analysis of disinformation [EB/OL]. [2020-12-21]. https://www.ideals.illinois.edu/bitstream/handle/2142/15205/fallis_{disinfo1}.pdf?sequence=2.

[10] KARLOVA N A, JIN H L. Notes from the underground city of disinformation: a conceptual investigation [C]//Proceedings of the American Society for Information Science and Technology. Seattle: ASIST, 2011.

[11] PAMMENT J. The EU's role in fighting disinformation: crafting a disinformation framework [EB/OL]. [2020-12-27]. https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720.

[12] SHU K, WANG S, LEE D, et al. Mining disinformation and fake news: concepts, methods, and recent advancements [EB/OL]. [2020-12-05]. https://arxiv.org/pdf/2001.00623.pdf.

[13] NATASCHA A K, KAREN E F. A social diffusion model of misinformation and disinformation for understanding human information behaviour [J]. Information research, 2013, 18(1): 573.

[14] RUBIN V L. Disinformation and misinformation triangle: a conceptual model for "fake news" epidemic, causal factors and interventions [J]. Journal of documentation, 2019, 75(5): 1013-1034.

[15] WANG Y G, CAI F Z, ENG K L, et al. A method for controlling disinformation propagation in social networks [J]. Journal of Computer Research and Development, 2012, 49(S2): 131-137.

[16] WU Y, LI Y N, ZHANG L. Disinformation propagation from a computational perspective: content, subjects, and patterns [J]. Journal of Henan Normal University (Natural Science Edition), 2019, 47(2): 29-35, 2.

[17] SMITH S T, KAO E K, MACKIN E D, et al. Automatic detection of influential actors in disinformation networks [J]. Proceedings of the National Academy of Sciences, 2020, 118(4): e2011216118.

[18] HUANG W H. Research and simulation on disinformation avoidance and filtering methods in sensor networks [J]. Computer Simulation, 2013, 30(6): 288-291, 427.

[19] WANG L, FENG S Y. Simulation of disinformation filtering methods for cloud computing [J]. Computer Simulation, 2018, 35(6): 211-214.

[20] HWANG Y, JI Y R, JEONG S H. Effects of disinformation using deepfake: the protective effect of media literacy education [J]. Cyberpsychology, behavior,

and social networking, 2021, 24(3): 188-193.

[21] ZHOU Y Q, JING Q, NIU Y. Research on library participation in disinformation governance under the background of "All-People Pandemic Response" [J]. Library and Information Service, 2020, 64(15): 177-183.

[22] JIANG J Y. Research on U.S. library participation in combating online disinformation [J]. Library Construction, 2018(12): 52-56, 62.

[23] HUANG Y T, FENG J. Disinformation identification from the perspective of information literacy: international progress and China's countermeasures [J]. Knowledge of Library and Information Science, 2021(2): 121-132.

[24] WANG J X. Reflections on public libraries' participation in information governance to improve public media and information literacy [J]. Digital Library Forum, 2020(5): 30-35.

[25] FALLIS D. What is disinformation [J]. Library trends, 2015, 63(3): 401-426.

[26] WOLVERTON C, STEVENS D. The impact of personality in recognizing disinformation [J]. Online information review, 2020, 44(1): 181-191.

[27] U.S. House of Representatives. National defense authorization act for fiscal year 2020: section 5323 on the encouragement of cooperative actions to detect and counter foreign influence operations [EB/OL]. [2021-01-12]. https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf.

[28] BRADLEY S. Securing the United States from online disinformation-a whole-of-society approach [EB/OL]. [2021-01-08]. https://carnegieendowment.org/2020/08/24/securing-united-states-from-online-disinformation-whole-of-society-approach-pub-82549.

[29] American 116th Congress. S.4499-COVID-19 misinformation and disinformation task force act of 2020 [EB/OL]. [2021-01-11]. https://www.congress.gov/bill/116th-congress/senate-bill/4499?r=1&s=1.

[30] RAND. Fighting disinformation online: a database of web tools [EB/OL]. [2021-01-11]. https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html.

[31] Atlantic Council. Digital forensic research lab (DFRLab) [EB/OL]. [2021-01-13]. https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/.

[32] MCFARLAND K. The new weapon of choice: technology and information operations today [EB/OL]. [2021-01-16]. https://isd.georgetown.edu/2020/10/21/isd-launches-new-report-on-information-operations/.

[33] European Commission. Code of practice on disinformation [EB/OL]. [2021-01-20]. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[34] European Commission. Action plan against disinformation [EB/OL]. [2021-01-21]. https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation.

[35] WANG Y F, CHEN M H, ZHAO K R, et al. Research analysis of national scientific and technological intelligence governance [J]. Information Studies: Theory & Application, 2018, 41(1): 5-8.

[36] ZHAO K R, WANG Y F. Research on capability perception of scientific and technological intelligence agencies [J]. Information Studies: Theory & Application, 2018, 41(1): 9-15.

[37] LONG L A. Activity-based intelligence: understanding the unknown known [J]. The intelligencer, 2013, 2(20): 7-15.

[38] WANG Y F, LIU J, CHEN M H, et al. Ecological perspective on intelligence governance [J]. Information Studies: Theory & Application, 2018, 41(1): 5-8.

[39] CHEN M H, CHEN F. Information ecology analysis of U.S. competitive intelligence system construction [J]. Information Studies: Theory & Application, 2018, 41(1): 9-15.

[40] ZHANG X J. Research on U.S. military intelligence theory [M]. Beijing: Military Science Press, 2011: 173.

[41] YAN L. Analysis of information ecological factors [J]. Journal of Intelligence, 2008(4): 77-79.

[42] WANG Y F, DU Y Q. Research path of intelligence perception integrating intelligence characterization [J]. Science and Technology Intelligence Research, 2020, 2(1): 1-11.

[43] HE G C. Establishing information early warning and rapid response systems to strengthen intelligence support [J]. Aerospace Industry Management, 2002(11): 28-29.

[44] PENG Y Q. Promoting modernization of the scientific and technological information governance system and governance capacity [J]. Digital Library Forum, 2020(5): 1.

[45] CHEN M H. Research on intelligence capabilities in national scientific and technological security governance [D]. Beijing: Peking University, 2020.

[46] LAN Y X, XIA Y X, LIU B Y. Modeling and simulation of online rumor propagation subjects oriented toward emergencies [J]. Information Science, 2018(5): 119-125.

Author Contributions: Chen Meihua: Paper writing; Wang Yanfei: Paper guidance and revision.

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