Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070901
ISSN 2371-8838 Vol. 7 Num. 9

Study on Cyberspace Governance in the Perspective of Digital Revolution

Jiehua Zhong

Faculty of Humanities and Social Sciences, Macao Polytechnic University, Macao, 999078, China

Keywords: Cyberspace governance; Social media; The digital age; Network security

Abstract: The mature development of online media has had a significant impact on the online space and real society. The great release of communication power and discourse power has shaped a decentralized communication pattern, bringing about complex phenomena in content generation and information dissemination. It has also brought real challenges and difficulties to the governance of the online space and society. This article focuses on the development and application of online space governance, starting from the source of public opinion guidance and management. It explores and analyzes the top-level design of the current online space governance mechanism, government-led management, platform main body responsibility, and self-organizing operation norms, and summarizes a comprehensive understanding of China's online space governance mechanism.

1. Introduction

The digital age refers to a historical stage in which humans expand their activity space and innovate development paradigms through continuous leaps in digital information technology. It is a historical summary of the current human development model[1-2]. The technological characteristics of the digital age make the interaction behavior of countries clearly influenced by two factors: uncertainty factors and changes in the international pattern, playing an important role in the transformative and continuous development of international relations[3]. The online space is a virtual reality space composed of "multiple domains," and the flow of data in the "multiple domains" based on the Internet is the new content of the online space. Unlike other similar concepts of cybersecurity, the cybersecurity of the digital age emphasizes the security issues brought about by spatial interaction and spatial integration[4].

Due to the technical deficiencies of cyberspace itself, the rule vacuum generated by the development of new technologies, and the disorder in competition among major powers, the security risks in cyberspace have become more generalized and compounded[5]. Cyber attacks, cybercrime, and activities of cyber terrorism are rampant. Unilateralism, protectionism, hegemonism, and power politics are on the rise. The situation of peace and security in cyberspace is becoming more severe, and the potential risks to human civilization from disruptive technologies are increasing. At the same time, the "digital divide" between countries and regions is widening, and the digital space is becoming a new high ground for major power competition and the seizing of international discourse power. The development among different countries and regions is increasingly imbalanced, and the dividends of the digital economy have failed to effectively benefit

the people of all countries[6]. Faced with the new situation, challenges, and threats in the development and governance of cyberspace, the international community must work together, consult and cooperate, and provide more just, reasonable, and effective solutions for the governance of cyberspace.

2. The Main Working Mechanism of Cyberspace Governance

2.1 Top-level Design Governance Mechanism

The concept of cyberspace governance originates from the discourse system guided by public opinion. Guiding public opinion is a unique and important concept in China's news and propaganda work. On January 24, 1994, national leaders first proposed at the National Conference on Ideological and Propaganda Work: "Correctly guiding public opinion is a very important task in the ideological and propaganda front." Since then, the concept of guiding public opinion has formally entered the top-level design of the Party and the country. Since the 16th National Congress of the Communist Party of China, national leaders have taken strengthening and improving governance capacity as the starting point and adhered to the scientific outlook on development as the guidance, incorporating "guiding public opinion" into the important proposition of governance capacity building, and putting forward a more perfect concept and approach of guiding public opinion. The decision adopted at the Fourth Plenary Session of the 16th Central Committee on September 19, 2004, pointed out that we must firmly grasp the orientation of public opinion and correctly guide social opinion. While giving full play to the role of traditional media, efforts should be made to promote the use and management of new media such as the Internet and mobile phone text messages, making them a new platform for ideological work and seizing the commanding heights of ideological and public opinion, and officially regarding the management and construction of the Internet as an important means of building a socialist harmonious society.

2.2 Government-led Management Mechanism

One is the continuous improvement of policies and regulations. With the increasing attention given by the country to the governance of cyberspace, relevant laws and regulations are also becoming more mature and complete. Currently, China's policies and regulations on Internet governance mainly include laws, administrative regulations, departmental rules, judicial interpretations, normative documents, and policy documents. Since the 18th National Congress, there have been two main internet laws, namely the "Cybersecurity Law of the People's Republic of China" and the "E-commerce Law of the People's Republic of China". The "Cybersecurity Law of the People's Republic of China" passed in November 2016, explicitly stipulates that the country advocates honest and trustworthy, healthy and civilized online behavior, promotes the dissemination of socialist core values, takes measures to improve the overall awareness and level of network security in society, and creates a good environment for the whole society to participate in promoting network security.

The second is the continuous improvement of working mechanisms. In February 2014, the Central Leading Group for Cybersecurity and Informatization was established to focus on national security and long-term development, and to coordinate and coordinate major issues related to cybersecurity and informatization in various fields such as economy, politics, culture, society, and the military. In March 2018, the Central Leading Group for Cybersecurity and Informatization was reformed into the Central Committee for Cybersecurity and Informatization, responsible for the top-level design, overall layout, coordination, overall promotion, and supervision and implementation of major work in the field of cybersecurity and informatization. The office of the

Central Committee for Cybersecurity and Informatization is the executive agency, mainly responsible for implementing the guidelines and policies for internet information dissemination and promoting the legal construction of internet information dissemination, guiding, coordinating, and supervising relevant departments to strengthen the management of internet information content, and playing an important role in regulating the order of internet communication and effectively guiding online public opinion.

Three is to vigorously support the construction of mainstream new media and government service accounts. Central and local key news units and government agencies, from different perspectives such as promoting media integration and innovative government services, actively promote the construction of mainstream media accounts and government service accounts, and continuously strengthen the mainstream public opinion position.

Four is to further strengthen management measures and efforts. In recent years, based on relevant laws, regulations, and departmental rules, law enforcement inspections have been strengthened, and the "Administrative Law Enforcement Procedures for Internet Information Content Management" and the "Guiding Opinions on the Work of Electronic Forensics of Internet Information Content Management Departments" and the "Guidelines for Electronic Data Forensics of Internet Information Content Management Departments" have been formulated and issued to provide legal basis and procedural guidance for administrative law enforcement. The administrative departments should carry out various special operations and activities, such as "cleaning up the internet", "sword net", and "cracking down on online pornography and illegal activities", and vigorously investigate a group of influential typical cases.

Five is to improve the mechanism for accepting online reports. The country has established a center for reporting illegal and harmful information, opened national network reporting hotlines, reporting websites, and reporting mobile apps in various regions. It has also formed teams of volunteers and volunteers for online reporting. In the reporting departments of the Internet Information Office in 31 provinces (autonomous regions, municipalities), and more than 2,000 websites, reporting hotlines have been opened. In 19 central news websites such as People's Daily, Xinhua News Agency, and CCTV, and more than 900 local news websites and commercial websites such as Qianlong.com, Sina.com, and Tianya.com, a "special zone for reporting harmful information online" has been set up to promote netizens' active reporting of harmful information online and active participation in comprehensive internet governance, and promote the co-construction, co-governance, and sharing of the cyberspace.

2.3 Platform Main Body Responsibility Mechanism

One is to play the main role and guide Internet companies to promote standardized management. Combining with the implementation of relevant laws and regulations, guiding Internet platforms to continuously improve a series of management systems such as real-name management, contract management, credit management, hierarchical management, review management, step management, and technical management, most platforms have formed a relatively complete main management system.

The second is the self-restraint mechanism of the platform. In July 2016, the director of the National Internet Information Office proposed the concept of "emphasizing basic norms, emphasizing basic management, strengthening territorial management responsibilities, and strengthening the responsibility of website subjects" at the meeting of the directors of the National Internet Information Office. Strengthening the main responsibility of website according to the principle of who organizes and who is responsible. The responsibility of supervision and self-discipline should be fulfilled by the network platform. It mainly includes executive

management standards, network platform editor responsibility system, content review system, network duty system, follow-up comment management system, user registration management system, etc. Strengthen the basic management, strengthen the main responsibility of the website, and improve the self-management level of the website platform.

The third is to improve the human-machine joint technology mechanism. Currently, network media often adopt algorithm recommendation to cater to audience needs, replacing manual review with technical algorithms. Algorithms become the gatekeepers who decide the information content that the audience receives, leading to the loss of strict review of recommended content, the proliferation of sensational and vulgar content, and some algorithm-based platforms relying solely on technical algorithms have had a negative impact on the orientation of online public opinion and the healthy dissemination of online content.

3. The Main Problems of Current Cyberspace Governance

Currently, China's governance of the cyberspace, especially the management mechanism of online media, has obvious disadvantages due to a late start. It is mostly in a state of post-follow-up and problem remediation. There are many aspects in terms of ideological concepts, policies and regulations, institutional mechanisms, model methods, and supervision and law enforcement that are not adapted.

3.1 Lack of coordination and foresight in policies and regulations, incomplete and unclear industry rules

Currently, the policies and regulations on cyberspace governance are relatively lagging behind and scattered, lacking effective coordination. First, legislation is relatively scattered. There are dozens of regulations and systems for the management of online media, involving multiple departments such as Internet information, industry and information technology, radio and television, culture, etc. Most of them are formulated based on departmental responsibilities, resulting in scattered industry management standards in different regulations and departments, making it difficult to form a system and lacking in concentration and authority. Second, the regulations are relatively lagging behind. The rapid development of emerging formats and the lagging behind of existing regulations have highlighted the contradiction. There are legislative gaps in some areas, which bring uncertainty to the industry's development. Some regulations and systems are introduced after the new applications and formats have gained momentum, resulting in the management of existing and incremental aspects being "difficult to handle," and even falling into the dilemma of "the tail is too big to fall." Third, the responsibilities and obligations between the government and enterprises are unclear and not detailed. Some Internet platform companies have become new entities for development, but there is a lack of clear regulations on which responsibilities the platforms should bear and how much responsibility they should bear. The government and enterprise governance responsibilities urgently need to be clarified. To some extent, the rapid iteration of online media applications has caused "creative destruction" to management, highlighting the ambiguity and lag of current laws and regulations. The lack of unified understanding of concept definitions and inadequate grasp of regular characteristics hinder the comprehensive and coordinated progress of governance work. The main reason is the insufficient forward-looking research on Internet technology and applications, and the lack of foresight, which leads to the management regulations not keeping up with technological development and application iterations.

3.2 Lack of Initiative in Platform Management and Limited Role of Industry Self-regulation and Social Supervision

Relying on platform management to promote industry self-discipline is the foundation of network media management. However, in practice, some network media platforms lack a strong sense of social responsibility and are not proactive or active in their management. There are even issues of engaging in gray areas or pushing boundaries to different extents. Some network media platforms have insufficient management resources compared to their user base. For example, the user base may range from tens of millions to billions, but the manual review team consists of only a few dozen people, making it difficult to ensure the quality of reviews. Although network media platforms have set up reporting platforms as required by regulatory authorities, the effectiveness of citizen reports is low, and the platform's handling of reports is also inadequate. This highlights the problems of ineffective reporting and lack of results. It also reflects the low enthusiasm of citizens in participating in online governance and the insufficient willingness of platforms to accept social supervision. At the same time, compared to foreign internet industry organizations, the role of internet industry organizations in China is limited, especially in terms of industry self-discipline, with low attention and insufficient frequency of activities. They lack authority, and their role in regulating the industry has not been effectively utilized. These problems result in a lack of basic support for network media management, with government departments relying more on mandatory regulations. However, there is insufficient internal self-regulation and a lack of a positive cycle.

3.3 Weak Management Base, Single Means and Inadequate Comprehensive Governance system

The current management of online media still has many problems. Firstly, there is a problem of "real name not matching real person" which undermines the real-name system. Issues of online media account impersonation, theft, and trading occur from time to time, especially the common buying and selling of self-media accounts. There has emerged a platform-based trading market online, where many accounts are "real name not matching real person". Secondly, there are limited management methods. The number of online media management objects is large, the industry types are diverse, and the business models iterate rapidly. It is difficult to adapt to the needs through governance methods relying on manpower. Online media has the characteristics of multi-point information dissemination, cross-platform, and covert propagation. Especially for the discovery and management of harmful information such as QR code drainage and private circle dissemination, it is difficult. Thirdly, there is a lack of capital management. Some of the current internet chaos is mainly caused by the deliberate pursuit of controversial topics and the creation of public opinion hotspots by "marketing parties". Most of these "marketing parties" are group actions, pursuing "number of followers" and "number of reads", driven by commercial capital. The infrastructure and system construction are the shortcomings that affect the effectiveness of management. It must be combined with development requirements, integrate concepts, organizations, systems, technologies, resources, and other aspects, further strengthen the management foundation, accelerate the pace of systematic planning and system construction, and comprehensively promote the construction of a comprehensive management system.

4. Policy Recommendations for the Management of Cyberspace security

The cybersecurity of the digital era has brought new challenges and opportunities to the country. Therefore, the country must be good at turning risks into opportunities and better respond to cybersecurity risks. China, as an emerging digital power and the largest developing country, must

make its mark in the digital era because only in this way can it better promote the development of international relations towards a more equitable direction. When addressing cybersecurity issues, both "soft" concepts and "hard" technical factors should be taken into account, while also paying attention to the main contradictions and historical trends, and continuously advancing in the face of challenges.

4.1 Empowering Network Security Protection with New Technologies and Concepts

Cutting-edge digital technology determines the boundaries and forms of cyberspace security. Therefore, research and development of cutting-edge technology will always be the most fundamental aspect of safeguarding cyberspace security. The laws of technological development show that the achievements of any technological progress can be applied to means of network attack or defense. In the digital era, a country's technological innovation capability plays an important role in safeguarding national security and enhancing international competitiveness. Especially in the early stages of internet technology architecture when security issues were not considered, a country can consider the security issues of new technologies during the research and development process of new digital technologies, plan ahead, and embed new technology and security standards into the technical architecture, so that the new technology system naturally has certain inherent security characteristics. In addition, investment in basic scientific research should be strengthened. Major breakthroughs in basic science have the potential to bring about "leapfrog" development in cyberspace security. The development of new generation artificial intelligence technology and quantum communication technology indicates that the scientific foundation on which digital technology research and development relies has far exceeded the scope of information and communication technology. The fusion development of basic disciplines such as mathematics, quantum physics, and new materials has become an indispensable force for the progress of digital technology. Therefore, only by increasing investment in the cross-disciplinary fusion development can we ensure the sustainable development of China's cyberspace and digital technology.

The administrative department should take the security concept as the core of strengthening national cyber resilience. Network security cannot be aimed at achieving absolute security. Most network attacks occur at the edge of national or social systems, and comprehensive network defense is neither realistic nor possible. The goal of network security is not to reduce network attack behavior to zero, but to limit malicious attack behavior within a certain range. Secondly, within the foreseeable range of network attacks, it is necessary to ensure that the losses of the attacked objects are within an acceptable range and have sufficient recovery capabilities, so as to have the "resilience" to withstand attacks. "Scope control", "loss control", and "recovery capability" are key aspects of the construction of network space security "resilience". China should actively explore the construction of the "zero-trust" framework of the Internet in the process of network technology development [7]. Zero-trust means that in network protection, there is no longer a distinction between inside and outside, friends and enemies, trusted and untrusted, but all devices, personnel, and networks are included in the scope of security verification. By covering the "zero-trust" architecture in the main aspects of network security, it can to a certain extent reduce the damage of network attacks to key areas and limit losses.

The administrative department should build an independent, complete, and secure supply chain system. The long chain of network security in the digital age is a great challenge for all countries. It involves not only the risk of "cut-off" in the supply chain struggle under traditional technological nationalism, but also the risk of network penetration and implantation of backdoors or viruses in various links of the supply chain. Unlike the pursuit of maximized interests in the industrial age's global division of labor, the severity of network security in the digital age requires that network powers must have complete and independent supply chain production capabilities in all areas from low-end to high-end.

4.2 Strengthening the Construction of Cybersecurity Systems in Key Areas

Data security has become the forefront of cybersecurity in the digital space. The core of various national cybersecurity threats is the misuse and manipulation of data. For example, the destruction of critical national infrastructure gradually relies on data interception and deletion as coercive measures. The manipulation of national political security also involves the illegal use of data. At the same time, artificial intelligence and algorithm security also heavily rely on data. It can be said that data security is a powerful entry point for solving cybersecurity in the digital age. It is the main contradiction in cybersecurity issues and a key area that tests a country's reform and governance capabilities. In addition, data security is also an important foundation for the development of the digital economy. Therefore, data security has increasingly become an urgent and symbolically significant security focus in cyberspace. Major digital powers and regions actively carry out legislation on data security. China has formed a data protection framework mainly based on the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. Next, specific practices in various fields and links should be further refined to form a security practice that is comprehensive, strict, flexible, and effective. For example, in the field of critical infrastructure protection, detailed data classification standards should be introduced as soon as possible, and special protection measures should be formulated for critical data. At the same time, in the field of digital economy, data sharing and flow should be strengthened to effectively address the dialectical relationship between data development and security. Under the overall framework of data legislation, active exploration should be made on the misuse of data based on artificial intelligence and algorithms, effectively mitigating the risk to national political security, and establishing a distinctive Chinese model for data security governance.

The administrative department should strengthen cybersecurity awareness and education with personal safety as the core. Individuals are the center and direct beneficiaries of cybersecurity. When individuals' awareness of cybersecurity risks increases, the overall situation of national cyberspace will naturally stabilize and develop. Therefore, in the process of promoting cybersecurity construction, China should increase the efforts of cybersecurity awareness and education for individual internet users through various channels, popularizing knowledge related to cybersecurity. Propaganda departments should inform the public of the latest cyberattack methods in a timely manner through case studies, especially various social engineering methods that mainly target individuals. Efforts should be made to popularize cybersecurity knowledge among young students, strengthen the guidance of online public opinion and ideological trends, maximize the cohesion of forces, and strengthen cooperation in various fields to maintain cybersecurity collectively.

4.3 Actively Participating in the Formulation of Cybersecurity Rules and Firmly Promoting International Cooperation

Strengthen cooperation with developing countries to narrow the digital divide. The digital divide has become an important factor affecting the balanced development of the digital age world. The United Nations has repeatedly mentioned that the digital divide may cause global uneven development of poverty and wealth, and it may also cause low digital countries to lose competitiveness in the online life of the "post-epidemic era", leading to a more difficult development situation. Scholars have also pointed out that in the era of artificial intelligence, developing countries may face the risk of "permanent marginalization" in the process of participating in the world economy and global division of labor [8]. As a new digital power and the largest developing country, China's concept of "a community with a shared future for mankind" carries a unique historical mission in the digital age. China should increase cooperation with developing countries in the digital economy, continue to promote the construction of the "Digital Silk Road", strengthen assistance to underdeveloped countries' digital infrastructure, and consider

the interests of developing countries when formulating international rules. Although it is not possible to effectively alleviate the challenges of global network security in the short term, reducing the digital divide is a basic foundation for making the cyberspace more secure in the long term.

Adhere to the United Nations as the core to promote the formulation of cybersecurity rules. The influence of "Western centrism" in international relations is constantly declining, and non-Western countries are increasingly not accepting an international order dominated by hegemony. The diversity of world civilization development is constantly highlighted. The Internet is a human symbiotic space that connects all spaces, all countries, and all civilizations. Therefore, the cyberspace rules of the digital age must be universal and representative, and must be formulated in the most legitimate multilateralism. In the short term, major digital powers still have strong motivation to implement unilateralism or formulate exclusive multilateralism policies in "small circles". However, in the long run, such cybersecurity policies will not bring true security. Network security must be solved jointly by all countries, so in the long run, it is an inevitable trend for countries to gradually return to the framework of the United Nations.

5. Conclusion

The cyberspace is a new space for human survival and national development. In this context, cyber governance has become a new component of national governance and global governance. Currently, with the support of related technologies, governing the cyberspace according to law and regulations is a necessary and urgent measure to maintain social harmony and stability, protect the legitimate rights and interests of citizens, and promote the healthy and orderly development of the cyberspace. The mature and widespread application of network media has brought profound impacts and changes to social relations and the cyberspace. On the one hand, the dissemination of network media endows the cyberspace with diversified participating subjects, multi-level governance objects, and dynamic dissemination processes. On the other hand, the complexity and systematicness of public opinion dissemination pose challenges and changes to the current cyberspace governance work. Based on this, it is necessary to enhance the governance capacity and means of the cyberspace, strengthen thinking updates, basic management, subject responsibility, and industry self-discipline, so as to fully enhance the dissemination power, guidance power, influence, and credibility of network media, and promote the continuous healthy and clear cyberspace environment.

References

[1] Liu Yangyue. Technological change and Cyberspace security Governance: Embracing the "era of uncertainty" [J]. Social Science, 2020 (09): 41-50.
[2] Liu Yangyue. Development trend and Governance of international security interaction in Cyberspace [J]. Teaching and Research, 2018 (01): 88-96.
[3] Lang Ping. Characteristics of network security competition among countries [J]. Strategic Decision Research, 2020, 11(02): 84-100.
[4] Liu Yangyue. Network Security in International Politics: Theoretical Perspectives and Arguments [J]. Journal of Foreign Affairs University, 2015, 32(05): 117-138.
[5] Zhou Hongren. The rise of cyberspace and strategic stability [J]. International Outlook, 2019, 11(03): 21-34.
[6] Lu Chuanying. Analysis of data and governance mechanism in Cyberspace [J]. Journal of Global Media, 2016, 3(04): 9-23.
[7] Jing Jiwu, Long Chun, Li Chang. Discussion on new trends of network security technology [J]. Frontiers of Data and Computing Development, 2019, 3(03):1-8.
[8] Gao Qiqi. The "risk of marginalization" and China's mission in the era of artificial Intelligence [J]. International Review, 2018(04): 38-50.