WHIOCE PUBLISHING PTE. LTD.
PROVIDING FIRST-CLASS SCIENTIFIC INFORMATION FOR TOP SCHOLARS

2025 Volume 3, Issue 4
Lecture Notes in Education, Arts, Management and Social Science
ISSN(Online): 2705-053X

The Historical Evolution and Future Prospects of China's Cyberspace Information Security Policies—From the Perspective of Historical Institutionalism

Yue Xie
SCU(Sichuan University), Chengdu 610000, Sichuan, China

Abstract: In recent years, cyberspace information security has increasingly occupied a vital position in the national security system, and its construction serves as a fundamental guarantee for China to become a cyberpower. Based on the analytical framework of historical institutionalism, China's cyberspace information security policies have gone through the embryonic, initial, growth, and acceleration periods. Under the macro-fields of stable political structure, reform-oriented economic system, and disruptive technological innovation, these policies have formed a path dependence dominated by the priority of science and technology and an encouraging development model. The stimulation of the external environment and the game among internal subjects constitute the driving forces behind their evolution. Looking at the history, China's cyberspace information security policies need to improve the supporting policy system, refine domain-specific and hierarchical regulations, and build a concomitant mechanism of technology-cyberspace-policy in the future.

Keywords: Cyberspace; Information; Security; Historical; Institutionalism; Future Prospect

Online publication: May 26, 2025

1. The Historical Process of China's Cyberspace Information Security Policies

China's cyberspace information security policies are inseparable from the development of the Internet. Policy formulation and implementation directly influence the structure and functions of the Internet, while the popularization of the Internet shapes the direction of policy-making. The evolution of these policies can be divided into four stages: embryonic, initial, growth, and acceleration, progressing from infancy to continuous improvement [1].

1.1. Embryonic Period: Computer System Security Era (Before 1990)

After personal computers became popular in the 1970s, computers were widely adopted for business processing, but computer networks remained undeveloped. Data transmission relied mainly on floppy disks, with limited functions, so threats primarily came from unauthorized access and information tampering. In the late 1980s, China accessed the international Internet. The establishment of the Computer Security Professional Committee in 1986 and the Information Security Department of the National Information Center in 1987 marked the beginning of China's computer security cause. Notable policies included the 1987 Draft Regulations on Computer Information System Security Protection and the 1988 formal regulations, but the system lacked unified standards and national management, focusing only on physical security

with limited anti-virus and anti-crime efforts [2].

1.2. Initial Stage: Information System Network Security Era (1990–2000)

The emergence of the Internet propelled information technology into a networking phase, integrating communication and computer security to ensure information confidentiality, integrity, and availability. Security products like firewalls and VPNs were adopted to combat threats. Inspired by global IT revolutions (e.g., the U.S. "Information Superhighway"), China accelerated informatization [3]. The 1994 Regulations on Computer Information System Security Protection was the first legal framework, followed by the 1999 establishment of the National Computer Network and Information Security Coordination Group. Policies like the 1994 Interim Provisions on International Networking Management and 2000 Internet Information Services Measures laid the groundwork, though they remained fragmented and lacked systematic design [4].

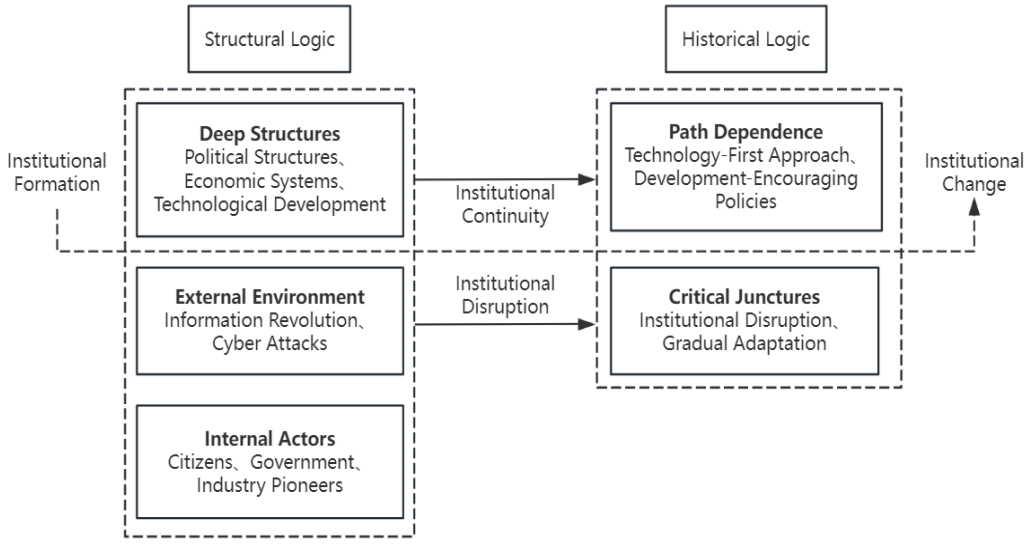

Figure 1. Analysis framework of the change of China's network information security policy

1.3. Growth Period: Cyberspace Security Era (2001–2015)

The concept of "cyberspace" emerged, and information security threats escalated from individual to state-level actors. Recognizing the need for dynamic management, China implemented the Information Security Level Protection System in 2007 ("Equal Protection 1.0"), and issued the Personal Information Protection Guide in 2013. The establishment of the Central Cyberspace Affairs Commission in 2014 and the first World Internet Conference marked a shift to strategic governance [5]. The 2015 Cybersecurity Law (public consultation) symbolized comprehensive legal construction, covering personal information protection and critical infrastructure, with policies integrating international standards and domestic realities.

1.4. Acceleration Period: Digital Space Security Era (2016–Present)

Since 2016, mobile Internet and technologies like 5G, AI, and blockchain have reshaped cyberspace, making information security a national security foundation[6]. The 2017 Cybersecurity Law established basic norms, followed by the 2021 Data Security Law and Personal Information Protection Law, which strengthened data protection and cross-border flow regulations. The Critical Information Infrastructure Security Protection Regulations further enhanced safeguards. With over 50 policies issued, China has formed a comprehensive, hierarchical policy system, though gaps remain in international cooperation, technical standardization, and implementation details.

1. The Historical Process of China's Cyberspace Information Security Policies

China's cyberspace information security policies are inseparable from the development of the Internet. Policy formulation and implementation directly influence the structure and functions of the Internet, while the popularization of the Internet shapes the direction of policy-making [7]. The evolution of these policies can be divided into four stages: embryonic, initial,

growth, and acceleration, progressing from infancy to continuous improvement.

2.1. Embryonic Period: Computer System Security Era (Before 1990)

After personal computers became popular in the 1970s, computers were widely adopted for business processing, but computer networks remained undeveloped. Data transmission relied mainly on floppy disks, with limited functions, so threats primarily came from unauthorized access and information tampering [8]. In the late 1980s, China accessed the international Internet. The establishment of the Computer Security Professional Committee in 1986 and the Information Security Department of the National Information Center in 1987 marked the beginning of China's computer security cause. Notable policies included the 1987 Draft Regulations on Computer Information System Security Protection and the 1988 formal regulations, but the system lacked unified standards and national management, focusing only on physical security with limited anti-virus and anti-crime efforts.

Table 1. China's Cyberspace Information Security Policies Before 1990

Year	Policy or Regulation Name	Description
1987	Draft Regulations on the Security Protection of Computer Information Systems	China's earliest regulations on information security, proposing basic principles and requirements for protecting computer information systems.
1988	Regulations of the People's Republic of China on the Security Protection of Computer Information Systems	Officially established the basic framework for information system security, including the classification of information systems and corresponding security protection measures.

2.2. Initial Stage: Information System Network Security Era (1990–2000)

The emergence of the Internet propelled information technology into a networking phase, integrating communication and computer security to ensure information confidentiality, integrity, and availability [9]. Security products like firewalls and VPNs were adopted to combat threats. Inspired by global IT revolutions (e.g., the U.S. "Information Superhighway"), China accelerated informatization. The 1994 Regulations on Computer Information System Security Protection was the first legal framework, followed by the 1999 establishment of the National Computer Network and Information Security Coordination Group. Policies like the 1994 Interim Provisions on International Networking Management and 2000 Internet Information Services Measures laid the groundwork, though they remained fragmented and lacked systematic design.

Table 2. China's Cyberspace Information Security Policies (1990-2000)

Year	Policy Name	Description
1994	Interim Provisions on the Administration of International Networking of Computer Information Networks of the People's Republic of China	Stipulated the management principles, access methods, security protection, and supervision of international networking of computer information networks.
1997	Administrative Measures for the Security Protection of International Networking of Computer Information Networks of the People's Republic of China	Clarified the management responsibilities for network security and strengthened the security protection of international networking of computer information networks.
1998	Regulations on the Administration of Internet Electronic Bulletin Services	Standardized Internet information service providers offering electronic bulletin services, emphasizing the security and legality of information content.
2000	Measures for the Administration of Internet Information Services	Stipulated the management principles of Internet information services, the responsibilities and obligations of service providers, and the management duties of relevant government departments.
2000	Regulations on Security Technical Measures for International Networking of Computer Information Networks	Proposed the security technical measures that must be observed in the use of international networking of computer information networks, enhancing the technical guarantee for network information security protection.

2.3. Growth Period: Cyberspace Security Era (2001–2015)

The concept of "cyberspace" emerged, and information security threats escalated from individual to state-level actors. Recognizing the need for dynamic management, China implemented the Information Security Level Protection System in 2007 ("Equal Protection 1.0"), and issued the Personal Information Protection Guide in 2013. The establishment of the Central Cyberspace Affairs Commission in 2014 and the first World Internet Conference marked a shift to strategic governance. The 2015 Cybersecurity Law (public consultation) symbolized comprehensive legal construction, covering personal information protection and critical infrastructure, with policies integrating international standards and domestic realities.

Table 3. Partial Cyberspace Information Security Policies of China (2001-2015)

Year	Policy Name	Description
2001	Notice of the State Council on Strengthening Network Information Security Management	Stipulated basic network security management responsibilities.
2003	Administrative Measures for the Security Protection of International Networking of Computer Information Networks	Specified security protection measures and requirements for international networking of computer information networks.
2004	Criteria for Classifying Security Protection Levels of Computer Information Systems	Classified the security protection levels of information systems and clarified the security protection requirements for each level.
2005	Electronic Signature Law	Stipulated the legal status and usage norms of electronic signatures.
2007	Administrative Measures for Network Security Level Protection	Formulated management measures for network security level protection.

2.4. Acceleration Period: Digital Space Security Era (2016–Present)

Since 2016, mobile Internet and technologies like 5G, AI, and blockchain have reshaped cyberspace, making information security a national security foundation. The 2017 Cybersecurity Law established basic norms, followed by the 2021 Data Security Law and Personal Information Protection Law, which strengthened data protection and cross-border flow regulations. The Critical Information Infrastructure Security Protection Regulations further enhanced safeguards. With over 50 policies issued, China has formed a comprehensive, hierarchical policy system, though gaps remain in international cooperation, technical standardization, and implementation details.

Table 4. Partial China's Cyberspace Information Security Policies Since 2016

Year	Policy Name	Description
2016	Cybersecurity Law	Established basic requirements for network security
2017	Notice on Strengthening Cyberspace Information Security Management	Strengthened personal information protection and standardized cyberspace information security management
2018	National Cyberspace Security Strategy	Clarified strategic objectives for cyberspace security defense, deterrence, and combat
2019	Personal Information Security Specifications	Standardized the collection and use of personal information to protect personal privacy
2020	Measures for Cybersecurity Review	Enhanced the security review of network products and services

2. The Evolutionary Logic of China's Cyberspace Information Security Policies

Based on the analytical framework of historical institutionalism, the evolutionary logic of China's cyberspace information security policies consists of deep structure, punctuated equilibrium, and dynamic mechanisms. Under the macro-contexts

of a stable political structure, reform-oriented economic system, and disruptive technological innovation, these policies have formed a path dependence dominated by technological priority and an encouragement-driven development model [10]. The stimulation from the external environment and the games among internal actors constitute the driving forces behind their evolution.

3.1. Deep Structure: Macro-context Analysis

Stable Political Structure: Unary Dominance and Pluralistic Coordination

China's political structure features "unary dominance with pluralistic coordination," where the central authority (core leadership of the Communist Party) ensures policy unity, while dynamic interactions among government agencies, social organizations, and public opinions enrich policy breadth [11]. This structure balances centralization with democratic participation, providing a stable yet adaptive political guarantee for policy evolution.

Reform-oriented Economic System: Centralized Unity and Market Regulation

The socialist market economy integrates market flexibility with state planning, enabling rapid policy responses to market changes while safeguarding national security [12]. It provides resources for the cybersecurity industry and stimulates enterprise innovation, balancing economic benefits with social stability to optimize cyberspace governance.

Disruptive Technological Innovation: Complementarity and Adaptive Updating

Technological iterations (e.g., cloud computing, AI) expand information dissemination but also breed cyber threats. This dual effect requires policies to adapt dynamically. For example, emerging technologies like big data demand innovative policy support to address data protection and privacy issues, forming a mutually reinforcing cycle between technology and policy [13].

3.2. Punctuated Equilibrium: Meso-level Institutional Analysis

Path Dependence on Technology-first Models

Policies exhibit strong path dependence on technology-driven development. Since the late 1980s, the state has prioritized IT R&D but lacked constraints on technological risks, often adopting a "patch-up" approach after technology deployment [14]. This strategy enhances national cybersecurity capabilities through technological innovation but has overlooked multi-dimensional coordination (e.g., legislation, international cooperation).

Key Turning Points

- 1994: Enactment of the first computer security law, marking legal breakthroughs.
- 1998: CIH virus outbreak prompted urgent cybersecurity legislation.
- 2014: Establishment of the Central Cyberspace Affairs Commission elevated cybersecurity to a national strategy.
- 2016: Implementation of the Cybersecurity Law standardized multi-subject responsibilities in cyberspace.

3.3. Dynamic Mechanisms: Micro-structural Analysis

External Environment: Technological Dividends and Threats

- Dividends: The digital revolution (e.g., big data, IoT) drives economic growth, forcing China to innovate technologically and formulate security policies [15].
- Threats: Overseas cyber warfare (e.g., advanced malware, state-sponsored attacks) targets critical infrastructure, necessitating continuous policy refinement.

Internal Interaction: Stakeholder Games

- Public-Government Dynamics: The public demands privacy protection amid big data abuses, while the government prioritizes cybersecurity, creating tensions that shape policy adjustments [16].
- Industry-Government Collaboration: The cybersecurity industry shifts from passive defense to proactive governance, requiring policies to balance security controls with technological innovation to foster industrial transformation.

4. Future Prospects of China's Cyberspace Information Security Policies

Against the backdrop of long-term institutional evolution, China's cyberspace information security policies need to shift from passive response to proactive engagement in attitude, from macro planning to local refinement in design, and from crisis-driven to technology-empowered in motivation [17]. These transitions will continuously improve the cyberspace security system and lay a solid foundation for building a cyberpower.

4.1. From Passive Response to Proactive Engagement: Enhancing Cybersecurity Policy Ecosystems

In the digital era, cyberspace security has become a global priority. Traditional policies relying on after-the-fact mitigation can no longer address evolving cyber threats. The future requires a fundamental shift to proactive governance：

- Preventive Framework: Build a robust system covering all potential risks, prioritizing proactive measures over reactive fixes. This requires anticipating unknown threats alongside defending known ones [18].
- Social Collaboration: Transform cybersecurity from a technical issue to a shared social responsibility. Policymakers should foster a cultural shift, guiding stakeholders—from enterprises to individual users—to participate in continuous, dynamic security maintenance.

The goal is a comprehensive ecosystem integrating technical protection, legal support, international cooperation, and public education to safeguard the digital landscape.

4.2. From Macro Planning to Local Refinement: Hierarchical and Domain-specific Legislation

China's cybersecurity framework has established top-level design ("four beams, eight columns"), but the next step is to refine implementation:

- Hierarchical Classification: Categorize network systems by security importance (e.g., national core networks vs. commercial systems) and apply differentiated protection measures [19].
- Domain-specific Regulation: Develop tailored policies for sectors like e-commerce, social media, and cloud computing, addressing unique risks. For example, enforce strict encryption for sensitive data (ID numbers, financial info) while relaxing controls for public information. This approach ensures policies are precise and effective, balancing security with practical needs.

4.3. From Crisis-driven to Technology-empowered: Constructing a Symbiotic Technology-Cyberspace-Policy Mechanism

Traditional crisis-response policies fail to keep pace with complex cyber threats. The solution lies in leveraging technologies like AI, big data, and quantum encryption to:

- Proactive Threat Detection: Use advanced tech for real-time monitoring and early risk identification, shifting from static to dynamic defense.
- Adaptive Policy Ecosystem: Build a symbiotic mechanism where policies adapt to technological advancements and cyberspace dynamics. This requires collaboration among policymakers, tech developers, and users to ensure policies are science-based and executable [20].

The ultimate aim is a human-machine-legal ecosystem where technology drives innovation, policies provide guidance, and human behavior reinforces security, promoting sustainable global cyberspace development.

Disclosure statement

The author declares no conflict of interest.

References

[1] Zhang Jing. Research on Cyberspace Information Security Control in the Big Data Era [J]. Shanxi Electronic Technology, 2024, (01): 119-122.

[2] Liu Heng, Wang Wei, Jin Wenhu, Han Yuan, Ma Jie, Zhao Wei. Cyberspace Information Security Issues and Countermeasures in the AI Era—Taking ChatGPT as an Example [J]. Cybersecurity Technology & Application, 2023, (11): 160-162.

[3] Deng Yu. Exploring China's Economic Development Prospects, Realistic Challenges and Transformation Path from an International Comparative Perspective [J]. Southwest Finance, 2023, (04): 32-45.

[4] Jing Wu. Discussion on the Development of Cyberspace Information Security in China [J]. Bulletin of the Chinese Academy of Sciences, 2022, 37(11): 1543-1545.

[5] Shao Guosong, Xie Jun. Development Status and Problems of Cyberspace Questionnaire Surveys in China [J]. Journal of Hunan University (Social Science Edition), 2021, 35(04): 149-155.

[6] Zhang Jin. Exploration on the Development Situation and Related Protection Technologies of Computer Cyberspace Information Security [J]. Modern Information Technology, 2019, 3(23): 139-141.

[7] Liu Boran, Wei Xiuming. US Cyberspace Information Security Strategy: Development Process, Evolution Characteristics and Essence [J]. Journal of Liaoning University (Philosophy and Social Sciences Edition), 2019, 47(03): 159-167.

[8] Lei Xin. Future Development Trends of Cyberspace Information Security [J]. Cable Television Technology, 2018, (08): 40-42.

[9] Liu Liang. Analysis of the Connotation of Cyberspace Political Security [J]. Journal of Central South University (Social Science Edition), 2016, 22(06): 142-148.

[10] Liu Mingxing, Zhang Dong, Shi Zonghan, Zhu Mengchang. The Power Structure of China's Political Elites and the Sustainability of Economic Decentralization [J]. China Economic Quarterly, 2016, 15(01): 289-320.

[11] Shan Chenggong. Discussion on Cyberspace Information Security Technology and Its Development Trends [J]. Electronic Technology & Software Engineering, 2013, (23): 225-226.

[12] Wu Aifang, Wu Wenjing. Global Cyberspace and Information Security Development Dynamics from 2003 to 2013 [J]. Information Security and Communications Privacy, 2013, (12): 48-56.

[13] Ding Changyan. The Transformation of Power Structure: The Foundation, Dimensions and Conditions of China's Political System Reform [J]. Journal of Yunnan Administration College, 2011, 13(06): 55-58.

[14] Yan Jinwu. On Cyberspace Information Policy [J]. Library and Information Service, 2004, (03): 26-31.

[15] Jiang Yaoping, Li Yijun, Wang Haiwei. International Comparative Study on National Cyberspace Information Security Strategic Planning [J]. Management Science, 2004, (01): 66-71.

[16] Song Xiaowen. Cyberspace Information Security in China [J]. New Technology of Library and Information Service, 2002, (01): 53-55.

[17] Jin, A., & Cheung, T. Cybersecurity Law in China: The Landscape. Journal of Cyber Policy, 2010.

[18] Zhang, L. The Evolution of Cybersecurity Policy in China. Journal of Information Security, 2015.

[19] Li, H., & Zheng, Y. Data Protection and Privacy under the Network Security Law in China. China Law Review, 2018.

[20] Wang, D., & Liu, H. The Impact of Cybersecurity Policy on Social Trust in China. Asian Journal of Communication, 2020.