International Journal Of History And Political Sciences

VOLUME Vol.06 Issue04 2026
PAGE NO. 35-40
DOI 10.37547/ijhps/Volume06Issue04-07

China's Experience in Ensuring Information Security Amidst the Development of Modern Technologies

Aliyev Jakhongir Erkinjon o‘g‘li
Phd Student, Tashkent State University Of Oriental Studies, Uzbekistan

Received: 26 February 2026; **Accepted:** 20 March 2026; **Published:** 14 April 2026

Abstract: This article analyzes the system of ensuring information security in the People’s Republic of China through a broad scientific approach. The main purpose of the study is to reveal why, in the Chinese experience, information security has gone beyond the scope of a simple technical protection issue and has evolved into a complex governance model closely connected with state sovereignty, political stability, social governance, control over data, regulation of platform activities, and support for the digital economy. The article examines China’s key legal documents, including the Cybersecurity Law of the People’s Republic of China, the Data Security Law of the People’s Republic of China, the Personal Information Protection Law of the People’s Republic of China), the Measures for Security Assessment of Cross-Border Data Transfer, the Regulations on the Security Protection of Critical Information Infrastructure, the Provisions on the Administration of Algorithmic Recommendation for Internet Information Services, and the Interim Measures for the Administration of Generative Artificial Intelligence Services. In addition, the article consistently analyzes China’s political and legal approaches to internet governance, in particular the principle of cyberspace sovereignty, the multilayered control system known as the Great Firewall of China, as well as the reasons behind the formation of local social media platforms and the domestic digital ecosystem.

Keywords: Information security, China, cybersecurity, cyber sovereignty, Great Firewall, data governance, platform governance, AI governance, digital sovereignty.

Introduction: In recent decades, the concept of information security has fundamentally expanded within global politics. While this term was previously associated primarily with protecting computer networks, restricting unauthorized access, and eliminating technical vulnerabilities, today it has evolved into a strategic concept inextricably linked to a state's political independence, economic competitiveness, technological sovereignty, and ability to govern society. The experience of China, in particular, demonstrates that the issue of control over the digital space is no longer merely an IT security problem but an integral component of the national development model. China's 2023 white paper, "China's Law-Based Cyberspace Governance in the New Era," states that the country views the law-based governance of cyberspace, maintaining order online, and protecting citizens' rights, while simultaneously ensuring national security and social interests, as a single, integrated task [1].

China's information security model differs significantly from the approach taken in Western countries. In the United States and the European Union, issues of internet governance are often analyzed within the framework of free speech, market competition, privacy, and the corporate responsibility of platforms. In China, however, the internet is primarily conceived as a space where state jurisdiction applies. For this reason, "网络主权" – or cyberspace sovereignty – holds a central place in China's official conceptual apparatus. The document "Sovereignty in Cyberspace: Theory and Practice (Version 2.0) " specifically outlines the state's right to independently choose its path of cyber development and to determine its internet

governance model and policies without external interference [2]. This document also explains legislative jurisdiction, administrative jurisdiction, judicial jurisdiction, and cyber defense as integral components of state sovereignty [2].

The relevance of this article is that China's information security model is often interpreted solely as "censorship" or "internet restriction." However, this model is far more complex, encompassing legal norms, technical filtering, platform governance, algorithmic control, data flow regulation, and the supervision of artificial intelligence services. Furthermore, the emergence of domestic social networks and local digital giants is not simply a result of protectionism, but rather a part of the state's political, economic, and security strategy. Therefore, the main research question is formulated as follows: Why and through what mechanisms has information security in China evolved into a comprehensive model of sovereign governance?

To answer this question, the article examines four key issues. First, it analyzes China's academic and theoretical concepts of information security. Second, it reviews the legal and regulatory framework that reinforces these concepts. Third, it studies practical mechanisms such as the Great Firewall, domestic platforms, and algorithm and AI governance. Fourth, it conducts a comparative analysis of the views of Chinese and foreign scholars on this model. In this way, the article seeks to move beyond a one-sided assessment of the Chinese experience and explain it as a multi-layered state strategy.

LITERATURE REVIEW AND RESEARCH METHODOLOGY

Scholarly perspectives on China's information security model are conventionally divided into two groups: the views of Chinese researchers and those of foreign researchers. Chinese scholars typically emphasize the interpretation of cyberspace sovereignty, the legitimate role of the state on the internet, and digital order as integral components of national security. Foreign researchers, in contrast, tend to analyze China's legal and regulatory framework, its practical implications, and its influence on the global internet order. A combined study of these two approaches is essential for a proper assessment of the Chinese model.

Huang Zhixiong holds a special place among Chinese researchers. He is known as a scholar affiliated with the Institute of International Law at Wuhan University and studies issues of international law in cyberspace [5]. In his article "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," co-authored with Kubo Mačák, Huang Zhixiong compares Chinese and Western views on the legal order in cyberspace [5]. According to him, China advocates for preserving the state's sovereign right in internet governance and explains the legal order on the internet from this very standpoint [5]. This approach is significant in explaining why China has chosen a "regulated internet" model over an "open internet."

Another important researcher from China is Lu Chuanying. He is a Senior Fellow at the Shanghai Institutes for International Studies and Deputy Director of the Institute for Public Policy and Innovation; his academic specialization is related to cybersecurity, cyber governance, and artificial intelligence regulation [6]. In Lu Chuanying's scholarly works, China's internet governance model is presented not merely as an internal control tool, but as a proposed alternative approach to the international cyber order [6]. In this respect, he explains China's cyber policy in the context of global normative competition.

Among foreign scholars, Rogier Creemers is one of the most frequently cited specialists. According to Leiden University, his research focuses on China's domestic digital technology policy and China's role in the global digital arena [7]. He has participated in the translation and commentary of several important Chinese laws and regulations within the DigiChina project [3], [4]. Creemers's work helps to understand the Chinese legal system not just as an instrument of superficial political control, but as a system linked to the internal logic of party-state governance.

The views of American scholar Graham Webster are also an important source for the study of China's digital policy. He serves as a research fellow in the Program on Geopolitics, Technology, and Governance at Stanford University and is the editor-in-chief of the DigiChina project [8]. Webster analyzes issues related to China's technology policy, US–China relations, and digital governance [8]. His work is particularly significant in explaining the practical implications of Chinese laws and regulations, especially in interpreting matters of algorithmic governance, personal data protection, and platform oversight.

Another American scholar, Samm Sacks, is one of the most cited foreign experts on China's data governance and cross-border data flows. According to New America and Yale Law School, she studies China's cybersecurity and data law system, US–China technological relations, and global data governance issues [9]. Her research in "The Evolution of China's Data Governance Regime" shows that the data governance system in China has been formed gradually but consistently [9]. Samm Sacks notes that China views data as a strategic resource and seeks to strengthen its sovereignty and

geopolitical interests by controlling it [9].

Rebecca Arcesati, a leading analyst at the MERICS think tank, deeply studies China's digital and technology policies, particularly data governance [10]. Her report "China's data management: Putting the party state in charge," co-authored with Jeroen Groenewegen-Lau, interprets China's data policy as a tool for expanding the control capabilities of the party-state [10]. This approach shows that data governance in China is not merely a security issue, but rather an integrated form of political governance and economic interests.

To summarize the existing academic literature, China's information security model is interpreted from two different perspectives. On the one hand, it is viewed as a system designed to ensure sovereignty, state governance, and internal stability. On the other hand, it is assessed as a controversial model that, in certain respects, imposes restrictions on internet freedom, data openness, and global information exchange. Therefore, when evaluating China's experience, neither a purely positive nor a purely negative approach is sufficient; it must be studied as a complex and multi-layered state policy.

This article was prepared using qualitative analytical and comparative methods. The official laws, regulations, and conceptual documents of China were selected as primary sources. Specifically, the "Cybersecurity Law" (中华人民共和国网络安全法), "Data Security Law" (中华人民共和国数据安全法), "Personal Information Protection Law" (中华人民共和国个人信息保护法), "Measures for Security Assessment of Data Cross-Border Transfer" (数据出境安全评估办法), the "Regulations on the Protection of Critical Information Infrastructure Security" (关键信息基础设施安全保护条例), the "Provisions on the Management of Algorithmic Recommendations in Internet Information Services" (互联网信息服务算法推荐管理规定), and the "Interim Measures for the Management of Generative Artificial Intelligence Services" (生成式人工智能服务管理暂行办法) were taken as the objects of legal analysis.

Materials from international research centers and expert platforms were used as secondary sources for the study. These included materials from DigiChina, New America, MERICS, Leiden University, Stanford University, and SIIS [7],[10]. These sources helped to explain the intrinsic content of the official documents, their political significance, and their interpretations in the international arena. In particular, these sources played a crucial role in interpreting the legal texts not merely as legal documents, but as governance mechanisms.

Methodologically, the research was conducted in three stages. The first stage involved a normative-legal analysis to examine the purpose, terminology, state-delegated powers, and regulatory principles of laws and regulations. In the second stage, a comparative analysis was used to contrast China's internet governance model with key Western approaches. The third stage employed an interpretive method to explain why China has created its own unique domestic internet space and system of local platforms, why it strictly controls data flows, and why it has integrated algorithms and artificial intelligence into its security framework. This method allowed the topic to be viewed not just as a collection of facts, but as a holistic model with its own political and legal logic.

RESULTS

The analysis revealed that the concept of information security in China is understood in a very broad sense. It is not merely about network security or combating malicious software. Instead, information security is understood in conjunction with cyberspace sovereignty, jurisdiction over data, critical infrastructure protection, personal data protection, platform activity oversight, and public opinion management [1],[4]. China's fundamental laws and policy documents reinforce this comprehensive approach.

The first key finding is that in China, cyberspace sovereignty is the central pillar of information security. The document "Sovereignty in Cyberspace: Theory and Practice (Version 2.0) " specifically outlines a state's right to independently choose its internet policy, its authority to determine the model of internet governance, and its right to conduct cyber defense [2]. According to this approach, control over the internet is considered a legitimate power of the state. Consequently, China views its internet space as a territory that must be protected from external influences. For this reason, internet order and security are prioritized over internet freedom.

The second key finding is that China's legal framework has been formed consistently and systematically. The Cybersecurity Law of the People's Republic of China regulates network security, critical information infrastructure, and order on the internet on a general basis [3]. This law defines its purpose as protecting cyberspace sovereignty, ensuring national security, and safeguarding social and public interests [3]. This indicates that the law is not a simple technical regulation but a political and legal document.

Additionally, the "Data Security Law" links data-related activities to the interests of state sovereignty, security, and development [4]. Article 1 of this law not only encourages the use of data but also establishes the protection of national sovereignty and security as a legal objective [4]. This approach signifies that data is viewed not just as an economic resource, but also as a security and geopolitical asset. Therefore, in China, data governance is not merely technical management but also a tool for protecting state interests.

Another important legal document, the "Personal Information Protection Law," appears at first glance to be a document that protects citizens' rights [11]. Indeed, it enshrines consent, the legal grounds for data processing, and certain rights related to personal information [11]. However, this law also covers issues of cross-border data transfer, foreign recipients, and international jurisdiction [11]. For this reason, the document is not just a law ensuring data security, but is also a component of state control over data.

A third significant outcome is that China has designated its critical information infrastructure as a distinct object of protection. The "Regulation on the Security Protection of Critical Information Infrastructure" places networks and digital systems in strategic sectors under a special protection regime [12]. The security of systems in energy, communications, transport, finance, public services, and other vital areas is regulated separately. This demonstrates that information security in China is not limited to content or data but also encompasses the stable operation of the entire digital infrastructure.

A fourth outcome is the strict regulation of cross-border data flows. According to the "Measures for Security Assessment of Cross-Border Data Transfers," a security assessment must be conducted before transferring certain types of data outside the country [13]. The document stipulates that the outbound transfer of critical and personal data could impact national security, economic stability, and public interests [13]. This approach indicates that China is not completely blocking the flow of data, but rather views it as a managed and state-controlled process.

The fifth finding is that China's decision to form its own distinct internet platforms and domestic digital ecosystem was a strategic one. Local platforms, including WeChat, Weibo, Douyin, Bilibili, and other services, not only grew under market conditions but also developed in an environment compatible with domestic jurisdiction, data control, and platform accountability systems [14]. A Tufts Digital Planet report indicates that Chinese platforms are tasked with maintaining social order, managing content, and acting in accordance with state requirements [14]. Therefore, China's distinct platforms are not merely economic products but are also part of its security and governance system.

The sixth finding is that the so-called "Great Firewall of China" is actually a multi-layered governance mechanism. Britannica describes this system as a combination of regulations and technological tools [15]. A USENIX study shows that it used DNS filtering, sending forged records, and other technical means [16]. However, this system does not consist solely of technical barriers. It also includes legal restrictions, platform licensing, content moderation, and governance tailored to state requirements. In this sense, the word "wall" takes on a more symbolic meaning; in practice, it is about maintaining a digital territorial border.

The seventh finding is that China has also made algorithms and artificial intelligence a matter of information security. The "Provisions on the Management of Algorithmic Recommendations in Internet Information Services" obligate platforms to establish security management for algorithmic recommendation systems, register certain services, and strengthen their accountability to users [17]. Meanwhile, the "Interim Measures for the Management of Generative Artificial Intelligence Services" stipulate that generative AI services must not produce outputs that are contrary to national security, social ethics, or public order [18]. This signifies that in China, the scope of information security has expanded to encompass the internal logic of content, algorithms, and artificial intelligence.

DISCUSSION

The findings indicate that China's information security model is based on three pillars: sovereignty, control, and development. First, the issue of sovereignty is the ideological foundation of the Chinese model. Huang Zhixiong and other Chinese researchers interpret cyberspace sovereignty as a natural extension of state sovereignty [5]. In this respect, China views the internet not as a free zone outside of international law, but as a space where national jurisdiction applies. This perspective explains why China is cautious regarding international platforms, why it prioritizes domestic political control in internet governance, and why it has imposed strict requirements on data flows.

Second, control is the practical core of the Chinese model. This control consists of more than just censorship or prohibitions. It signifies a comprehensive governance system that includes the special protection of critical infrastructure, the imposition of legal obligations on platforms, data categorization, data flow

assessment, algorithm registration, and the regulation of artificial intelligence services [12]. For this reason, the Chinese model manifests as a more centralized and governance-oriented system.

Thirdly, the issue of development is another crucial part of the Chinese model. China's internet policy is often interpreted solely in the context of restrictions. In reality, the state also places great importance on developing domestic platforms, utilizing data as an economic resource, supporting local technology companies, and strengthening the internal pillars of the digital economy [14]. Therefore, evaluating the Chinese model as purely repressive or purely protectionist would be one-sided. It is a state strategy that combines control with development.

The analyses of Rogier Creemers and Graham Webster show that in Chinese legislation, the concepts of "security" and "healthy development" are not juxtaposed [7], [8]. On the contrary, security is viewed as a necessary precondition for progress. This situation differs from the conflicting interpretation of "freedom versus security" in the West. China operates more under a "development under control" model. For this reason, China's distinct internet ecosystem both maintains internal order and supports national economic interests.

However, the model has serious controversial aspects. First, a broad interpretation of the concepts of security and political stability could narrow the space for independent information exchange. Second, complex requirements for transferring data abroad create additional barriers for international business, scientific cooperation, and digital innovation. Samm Sacks also points out that while China's data management system is robust, in practice, it increases uncertainty and regulatory costs [9]. Rebecca Arcesati argues that the strengthening of party-state control over data reinforces political centralization [10].

Nevertheless, there are aspects that can be learned from China's experience. In particular, protecting critical information infrastructure, categorizing data, assessing cross-border data flows from a security standpoint, strengthening the social responsibility of platforms, and introducing initial security criteria for artificial intelligence services are also of practical importance for other countries. However, such an approach should not be copied wholesale but should instead be adapted to the national legal environment, civil liberties, and international integration requirements.

CONCLUSION

In China, the information security framework is not limited to protection against cyberattacks or the implementation of technical security measures. This system is considerably broader and more complex, encompassing interconnected areas such as strengthening state sovereignty, maintaining political stability, tightening control over data, regulating digital platforms, protecting critical information infrastructure, and managing digital economy processes. From this perspective, information security in China is not merely a narrow technical concept but rather a vital component of state governance, national security, and digital development policy. For this very reason, the legal foundations of this model have been systematically established, including the Cybersecurity Law of the People's Republic of China, the Data Security Law, the Personal Information Protection Law, the Measures for Security Assessment of Cross-Border Data Transfers, the Regulation on the Security and Protection of Critical Information Infrastructure, as well as rules governing algorithmic recommendations and generative artificial intelligence.

China's creation of its own unique domestic digital space and national social media system is also directly linked to this strategic approach. This is not merely about restricting foreign platforms. In fact, this policy aims to keep data within the country's jurisdiction, develop local platforms that operate in compliance with state requirements, protect the domestic digital market, and reduce technological dependence on external factors. Therefore, China's digital policy can be said to be built on the principles of national interest, security, and technological independence. In this process, the often-mentioned "Great Firewall of China" functions not as a simple technical blocking tool, but as a complex and multi-layered control system that combines technical, legal, and administrative mechanisms.

Based on this study, it can be concluded that the Chinese model represents one of the most centralized, systematic, and consistent forms of information security policy today. Its strength lies in providing the state with a high degree of control over data flows, digital platforms, and strategic infrastructure. Consequently, the state is able to respond more rapidly and centrally to risks and threats in the digital space. However, these very features also give rise to the model's most controversial aspects. This is because such an approach is sparking various debates regarding internet freedom, information transparency, user rights, and international data exchange. Therefore, while China's experience is notable on one hand as an effective governance model, on the other, it is also regarded as a restrictive system in matters of digital freedom and openness.

From this perspective, the Chinese experience is

significant for Uzbekistan, and for Central Asian countries in general, not as a ready-made template to be copied in its entirety, but as a practical model that can be thoroughly studied in specific areas. In particular, certain lessons can be drawn from China's approach to issues such as protecting critical information infrastructure, legally regulating data handling, strengthening platform liability, ensuring personal data security, and increasing national digital resilience. Most importantly, any foreign experience must be selectively applied and adapted in harmony with national conditions, the legal environment, societal needs, and the principles of an open information space. Only then can such experience yield practically beneficial results.

REFERENCES

1. Arcesati, R., & Groenewegen-Lau, J. (2023). China's data management: Putting the party-state in charge. MERICS.
2. Creemers, R. (2018). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). DigiChina.
3. Creemers, R. (2022, January 10). Translation: Internet Information Service Algorithmic Recommendation Management Provisions (Effective March 1, 2022). DigiChina.
4. Creemers, R., Sacks, S., & Webster, G. (2021, August 18). Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021). DigiChina.
5. Cyberspace Administration of China. (2020, November 25). Sovereignty in cyberspace: Theory and practice (Version 2.0).
6. Cyberspace Administration of China. (2023, July 13). Interim Measures for the Management of Generative Artificial Intelligence Services [生成式人工智能服务管理暂行办法].
7. DigiChina. (2021, June 29). Translation: Data Security Law of the People's Republic of China.
8. DigiChina. (2021, November 1). Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021).
9. DigiChina. (2022, July 8). Translation: Outbound Data Transfer Security Assessment Measures (Effective Sept. 1, 2022).
10. Encyclopaedia Britannica. (n.d.). Great Firewall.
11. Hoang, N. P., Niaki, A. A., Dalek, J., Knockel, J., Lin, P., Marczak, B., Nishihata, M., Gill, P., & Polychronakis, M. (2021). How great is the Great Firewall? Measuring China's DNS censorship. In 30th USENIX Security Symposium (USENIX Security 21).
12. Huang, Z., & Mačák, K. (2017). Towards the international rule of law in cyberspace: Contrasting Chinese and Western approaches. Chinese Journal of International Law.
13. Lu, C. (n.d.). Profile and research materials on cyber governance. Shanghai Institutes for International Studies (SIIS).
14. Sacks, S. (n.d.). Profile and analyses on China's data governance. New America; Yale Law School, Paul Tsai China Center.
15. Stanford University. (n.d.). Graham Webster. Stanford Profiles.
16. The State Council Information Office of the People's Republic of China. (2023, March 16). China's law-based cyberspace governance in the new era.
17. Wang, J. (2022). Platform responsibility with Chinese characteristics. Digital Planet, The Fletcher School, Tufts University.