AN UNBREAKABLE WALL?

Challenges and Prospects of Defending Freedom of Information in China

RESILIENCE INNOVATION LAB

An Unbreakable Wall? Challenges and Opportunities of Defending Freedom of Information in China

Enquiry: info.ril@proton.me

An Unbreakable Wall? Challenges and Opportunities of Defending Freedom of Information in China

TABLE OF CONTENTS

About Us

Resilience Innovation Lab (RIL), founded by Asian veteran researchers and human rights defenders in 2023, serves to promote innovation, experimentation, and the exchange of research and educational initiatives that aim to develop and strengthen the democratic and digital resilience of organisations and individuals working in repressive environments.

RIL envisions a synergy of democracy, technology and civil society resilience today, especially when authoritarianism emerges as a common threat to liberal democracies and open societies. Building the capacities of citizens and civil groups to respond to such a new environment with creative and innovative instruments is of paramount importance for their sustainable development.

RIL focuses on researching Web3 technology, digital preservation of collective memory and history in conflict and post-conflict areas, resilience of information freedom and of rule of law institutions as well as rule of law cultures in non-democratic regimes.

Official website:

Subscribe our newsletters:

Executive Summary

Over the past decade, China's information environment has significantly deteriorated due to increasing state control over digital communication. Notable intensifications of censorship and surveillance coincided with major events, including the 2019 Hong Kong protests, the COVID-19 pandemic in 2020, and the White Paper Movement in 2022. The Chinese Communist Party (CCP) has systematically tightened its grip on cyberspace, driven by concerns about foreign ideological influence and domestic regime security.

The CCP's approach includes extensive digital surveillance, narrative control through media manipulation, and reinforced digital border controls such as the Great Firewall. Recent legislative developments, including amendments to national security laws and new cybersecurity regulations, further restrict information flows, impacting businesses, journalists, academics, and civil society.

Businesses, especially multinational corporations, face heightened risks due to China's increasingly restrictive digital environment. Due diligence operations have been severely limited, with entities experiencing raids, exit bans, informal governmental warnings, and restricted access to crucial corporate information databases.

Civil society organisations, journalists, and academics are similarly constrained, facing routine surveillance, censorship, and significant operational disruptions. Academic freedom, journalistic independence, and civic activism are persistently challenged by vague legal boundaries, intensified surveillance practices, and direct threats from authorities.

Looking forward, the information freedom outlook in China remains concerning. Escalating geopolitical tensions, economic uncertainties, and the CCP’s deployment of artificial intelligence for surveillance purposes are expected to deepen information

control. The erosion of conventional mitigation frameworks, exemplified by the decline of Hong Kong's autonomy, further compounds these challenges.

Policy Recommendations:

- National governments should incorporate digital rights clauses into diplomatic engagements and trade agreements, supported by annual assessments of China's digital policies.
- Multilateral institutions (WB, IMF, WTO) must establish regulatory standards emphasising open information access and enhance mechanisms monitoring China's digital repression.
- Businesses should conduct continuous risk assessments, facilitated by Chambers of Commerce and industry associations, adopting a Business and Human Rights Charter to align with global human rights standards.
- Civil society, media, and academia should proactively preserve at-risk information, establish international collaborations, and develop strategies to counteract censorship, thus safeguarding historical and contemporary records for future generations.

1. Introduction

Over the past decade, the information environment in the People's Republic of China (hereafter China) has markedly deteriorated, characterised by systematic tightening of state control over the dissemination and accessibility of information. This worrying trend was particularly pronounced during three pivotal events: the Hong Kong protests in 2019, the COVID-19 pandemic in 2020, and the White Paper Movement in 2022. Each event triggered intensified censorship, enhanced surveillance, and proactive state-led narrative management, reflecting the Chinese government's heightened resolve to centralise information control and limit public discourse.

The 2019 Hong Kong protests, initially sparked by a controversial extradition bill, represented a significant turning point. Chinese authorities swiftly exerted extensive control over information flows to prevent supportive sentiments from spreading to the mainland. Closely following these events, the global outbreak of COVID-19 in early 2020 saw Chinese authorities heavily censoring information regarding the virus's origins, the government's management of the crisis, and public criticism. This stringent approach not only affected the effectiveness of public health responses but also underscored the government's escalated commitment to crisis management through rigorous information manipulation. Similarly, during the White Paper Movement of 2022—a widespread response to stringent COVID-19 restrictions—authorities once again intensified surveillance and censorship, swiftly curtailing any organised dissent by tightly controlling both digital and physical public spaces.

Looking ahead, the prospects for information freedom remain challenging. China's digital space is becoming increasingly isolated from the global digital ecosystem, a situation reinforced by the sophisticated system known as the "Great Firewall." This isolation has resulted in an echo chamber, limiting Chinese citizens largely to state-approved narratives and significantly distancing them from global perspectives. Moreover, the rapid advancement and implementation of artificial intelligence (AI) technologies are poised to dramatically enhance the Chinese state's

surveillance, censorship, and narrative-shaping capabilities. AI-driven systems offer unprecedented capabilities for real-time monitoring, content filtering, and information manipulation, thereby significantly amplifying the government's power to control domestic information flows and shape public opinion.

Politically, China's increasingly restrictive information policies are driven by two primary motivations. Firstly, the Chinese Communist Party (CCP) seeks to isolate China's cyberspace from external influences, particularly Western ideologies that the regime regards as threats to its political stability. Secondly, by rigorously managing public narratives, the government aims to consolidate state authority and ensure political conformity—objectives central to President Xi Jinping's broader agenda of reinforcing CCP dominance and his own leadership.

A free and transparent information environment is critically important for several reasons. Democratic accountability and effective governance fundamentally depend on citizens having access to accurate, diverse, and uncensored information. Informed public discourse enables citizens to hold governments accountable, thereby enhancing transparency and reducing opportunities for corruption. For businesses, transparent information environments underpin informed investment decisions, risk mitigation, fair competition, and overall market stability. Conversely, authoritarian regimes typically restrict the free flow of information, resulting in ideologically bounded rationality. Such regimes often limit information dissemination to appease ruling elites and prevent political repercussions, consequently impairing effective governance, economic strategy, innovation, and global competitiveness.

This report comprehensively documents the information environment in China under the rule of the Chinese Communist Party, particularly emphasising developments since President Xi Jinping's rise to power. It critically analyses the ways in which systematic, state-led efforts to control and manipulate information affect various segments of society—including the information supply chain, public access to information, and operational conditions for businesses (especially within the due

diligence industry), civil society organisations, journalists, and academics either operating in or dealing with China. Through evidence-based insights from multiple perspectives, this report aims to inform stakeholders—from policymakers and international businesses to civil society groups and academic institutions—and encourages collaborative efforts to address challenges in China's information environment and related global information networks. Ultimately, this comprehensive analysis seeks to enhance understanding of the complex dynamics shaping China's information landscape and to facilitate constructive dialogue and coordinated action aimed at fostering greater openness, transparency, and resilience against all forms of information manipulation.

The Resilience Innovation Lab acknowledges the invaluable contributions of several anonymous contributors and interviewees who have opted not to disclose their identities due to safety and security concerns. Their courage and insightful perspectives have significantly enhanced the depth and authenticity of this report. It is our sincere hope that, in the near future, contributors and researchers will no longer feel compelled to conceal their identities but will instead openly participate in advocating for a free, transparent, and open society in China.

2. Information Environment in the People's Republic of China: An Overview

2.1 Xi's Emphasis on PRC's Cyber Sovereignty

> *"The principle of openness as norm and non-disclosure as exception … promoting the digitalisation of government transparency, enhancing online government information and data service platforms."*
>
> *The Fourth Plenary Session of the 18th Central Committee of the Communist Party of China*[1]

The quotation above is taken from President Xi Jinping's speech delivered on 28 October 2014. In this address, Xi emphasised the importance of opening the government to public scrutiny as a cornerstone of his plan to promote "rule-based governance" in China. He asserted that government transparency could serve as a significant catalyst for eradicating corruption during his first term in office. At the time, many Western observers were optimistic about Xi's potential as a reform-oriented leader who might further China's openness to the world.

Nevertheless, the full scope of Xi's intentions proved far broader than initially anticipated. While publicly positioning himself as an advocate of rule-based governance, Xi's anti-corruption campaign primarily targeted his political rivals. Concurrently, he mobilised various apparatuses within the Chinese Communist Party (CCP) and government institutions to establish significantly tighter control over public information—determining what information is accessible, how it can be accessed, and who can access it. Over time, it became evident that Xi's principal political objectives were

[1] "中共中央关于全面推进依法治国若干重大问题的决定 [CCP Central Committee Decision concerning Several Major Issues in Comprehensively Advancing Governance According to Law]," *The State Council, The People's Republic of China*, Oct 28 2014, accessed Mar 28 2025, https://www.gov.cn/zhengce/2014-10/28/content_2771946.htm

consolidating his own authority and reinforcing the CCP's control over the Chinese population. To enhance social and political control, securing data in the digital world as the new strategic resources is essential. Strengthening the CCP's dominance over cyberspace for the sake of warranting control over digital data emerged as a crucial component of his broader strategy to safeguard national security.

In February 2014, President Xi Jinping chaired the inaugural meeting of the Central Cybersecurity and Informatisation Leading Group (中央网络安全和信息化领导小组), a party committee responsible for overseeing China's newly established executive agency for cyber-related issues—the Cyberspace Administration of China (CAC, 中央网络安全和信息化委员会办公室). Unlike typical CCP leading groups, which are usually chaired by the state Premier, Xi appointed himself chairperson to ensure direct oversight of the group's initiatives. Xi intended the Leading Group and the CAC to be at the forefront of developing and implementing the comprehensive cybersecurity strategy under his personal guidance.[2] This arrangement allowed Xi to directly shape China's cyber legislation, ensuring close alignment with his broader political objectives.

According to Wakako Ito, Director of The Japan Forum on International Relations, who specialises in research on China's cyber governance, Xi Jinping was the first Chinese leader to explicitly incorporate cybersecurity into China's national security framework, effectively placing cybersecurity among the nation's highest priorities. Ito highlights two main objectives underpinning Xi's emphasis on 'cyber sovereignty.' Firstly, Xi aims to prevent foreign interference—particularly from the United States—in China's digital environment. This became particularly evident during the US-China trade war under the first Trump administration, when Xi mobilised extensive national security and legislative resources to restrict American access to Chinese cyberspace and data.

[2] Max Parasol, "The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams," *Computer Law & Security Review 34*, no. 1 (2018): 72.

Secondly, Xi seeks to establish a comprehensive framework that enables the regime to exercise tighter control over domestic cyberspace.[3]

> *"There is no national security without cybersecurity."*
>
> *The Cyberspace Administration of China*[4]

China has a long-standing history of censoring online information through the "Great Firewall," which prevents citizens from accessing overseas content deemed unfavourable to the Chinese Communist Party's (CCP) rule, particularly when domestic discussions might appear provocative to the regime. Nevertheless, this marks the first instance in which cybersecurity has been explicitly prioritised as a central component of national security and sovereignty.

Two years after Xi Jinping's initial emphasis on placing cybersecurity at the core of national security, the Cyberspace Administration of China (CAC) issued its first guiding policy document in December 2016. Titled the *National Cyberspace Security Strategy* (国家网络空间安全战略), the document outlines the strategic objectives of the Chinese Communist Party (CCP) regarding cyber governance, aligned closely with the principles articulated by President Xi. The strategy underscores the complex cybersecurity landscape and identifies cyberspace as a critical domain of national sovereignty, vulnerable to manipulation by external forces intent on interfering with domestic politics, destabilising China's political system, inciting social unrest, subverting the regime, and conducting cyber espionage. Consequently, from the CCP's perspective, it is crucial for the Chinese government to implement robust legislation,

---

[3] Wakako Ito, "The State-Oriented Model of Internet Regulation: The Case of China," *Public and Private Governance of Cybersecurity: Challenges and Potential*, (2023): 41.

[4] "国家网络空间安全战略 [Cyberspace Security Strategy]," *Office of the Central Cyberspace Affairs Commission, Cyberspace Administration of China*, Dec 27 2016, accessed 28 March 2025, https://www.cac.gov.cn/2016-12/27/c_1120195926.htm

regulatory frameworks, and policy measures to mitigate cybersecurity risks, thus ensuring national security and protecting China's sovereignty from external interference.[5]

Although the Strategy includes a section highlighting opportunities presented by rapid economic growth, its core emphasis remains firmly on countering threats emerging from cyberspace and penalising any actors seeking to undermine the regime through cyber activities. This cautious stance reflects Xi Jinping's overall approach towards the development and governance of cyberspace.

The concept of cyber sovereignty, combined with President Xi's promotion of a "holistic view of national security" and his emphasis on advancing "rule-based governance" in China, has led to a series of legislative actions aimed at enhancing cyber control. The following sections highlight how the Chinese state has employed existing legal instruments and introduced new regulatory frameworks explicitly designed to "safeguard cybersecurity."

2.2 Reinforcing Existing Regulations

After establishing the relevant institutional apparatus and outlining a legislative blueprint, President Xi Jinping laid the groundwork for a comprehensive legal framework aimed at significantly tightening the regime's control over cyber activities. Xi adopted a dual-track approach: revising existing laws and introducing new, tailor-made legislation to regulate cyberspace. Under his leadership, three existing laws were amended—the National Security Law, the Counter Espionage Law, and the Guarding State Secrets Law. In parallel, three new pieces of legislation and one key regulation were introduced to directly address emerging cyber threats: the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the recently passed Network Data Security Management Regulation, which is scheduled to come into effect in 2025.

[5] Ibid.

Together, these legislative efforts form an overarching framework designed to control information flows under the banners of national security and data protection.

2.2.1 National Security Law (NSL)

The amended National Security Law (NSL) provides a comprehensive legal foundation for China's national security framework. The revised NSL explicitly incorporates provisions related to cybersecurity, with its language reflected in subsequent cyberspace-focused legislation and frequently cited in legal cases involving digital security. The law underscores the imperative for China to strengthen its capacity to protect the information security of critical infrastructure. It mandates the prosecution of cyber-related offences, including cyberattacks, unauthorised intrusions, data theft, and the dissemination of illegal or harmful information by actors seeking to exploit cyberspace to destabilise the regime.[6]

2.2.2 Counter Espionage Law (CSL)

When the Counter Espionage Law (CSL) was first enacted in 2014, analysts and observers raised concerns over its vague language and the broad definition of espionage. These concerns deepened significantly following the 2023 amendment by the Standing Committee of the National People's Congress (SCNPC), particularly in light of the subsequent arrest of a notable number of foreign nationals in China. The revised CSL expanded the already ambiguous definition of espionage to include the collection or handling of any "documents, data, materials or items related to national security"—a categorisation open to wide interpretation by China's national security authorities. Significantly, the amended law explicitly lists cyberattacks on China's

[6] "中华人民共和国国家安全法 [National Security Law of the People's Republic of China]," *The State Council, The People's Republic of China*, July 1 2015, accessed Mar 28 2025, https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

information infrastructure as a form of espionage, signalling a sharpened legal focus on cybersecurity within the broader national security framework. [7]

According to the Japanese news outlet Kyodo News, China has detained 17 Japanese nationals since 2014. Among them is an employee of the pharmaceutical company Astellas Pharma, who has been held since March 2023 on suspicion of espionage.[8] As trials related to national security laws in China are conducted behind closed doors, it is difficult to determine whether this particular case is directly linked to cybersecurity.[9] Nonetheless, the amended Counter Espionage Law (CSL) now encompasses cyber activities and data transfers within its expanded definition of espionage, creating significant uncertainty for the business community operating within China.

2.2.3. Guarding State Secrets Law (GSSL)

Following the amendment of the Counter Espionage Law (CSL) in February 2024, the Standing Committee of the National People's Congress (SCNPC) continued its efforts to broaden the scope of espionage and redefine state secrets through the amended Guarding State Secrets Law (GSSL). Reflecting President Xi Jinping's broader strategy to assert the Chinese Communist Party's (CCP) authority over the state, the revised GSSL explicitly positions the CCP as the principal actor responsible for safeguarding state secrets. It entrusts the Party with leading and coordinating legislative efforts across all levels of government in the realm of information and state secrecy.

---

[7] Simone McCarthy & Nectar Gan, "China has widened its already sweeping counter-espionage law. Experts say foreign business should be worried," *CNN Business*, Apr 27 2023, accessed Mar 28 2025, https://edition.cnn.com/2023/04/27/china/china-counter-espionage-law-revision-intl-hnk/index.html

[8] "Japan demads release of national detained in China for espionage," *Kyodo News*, Mar 27 2023, accessed 28 Mar 2025, https://english.kyodonews.net/news/2023/03/43bc3ac94d9d-japan-demands-release-of-national-detained-in-china-top-spokesman.html

[9] "Japan's Astellas says employee indicted by China's prosecutors," *Reuters*, Aug 21 2024, accessed 28 Mar 2025, https://www.reuters.com/business/healthcare-pharmaceuticals/japans-astellas-says-employee-indicted-by-chinas-prosecutors-2024-08-21/

The amended GSSL not only retained the broad definition of a "state secret"—defined as "information that can endanger national security"—but also continued to grant wide discretion to the national security apparatus in interpreting and enforcing the law. Furthermore, the amendment laid the groundwork for future legislation concerning so-called "work secrets," referring to information that does not meet the threshold of a state secret but could cause "adverse effects if disclosed."[10] Given the ambiguity surrounding what constitutes either a state secret or a work secret, it is extremely difficult for individuals and organisations to determine what information is legally permissible to share. As a result, the SCNPC has created a chilling effect across sectors, with entities operating in China increasingly inclined to withhold information or deny access to data—particularly across borders. This, in turn, has contributed to the ongoing deterioration of information freedom.

2.3 Creation of a new legal framework for cyber governance

2.3.1 Cybersecurity Law (CL)

In November 2016, the Standing Committee of the National People's Congress (SCNPC) passed the first landmark legislation forming the cornerstone of China's cyber governance framework—the Cybersecurity Law (CL). One of its most controversial provisions is the legal requirement for data localisation, which mandates that operators of "critical information infrastructure" must store data collected and generated within China's borders.[11] The CL defines "critical information infrastructure" broadly, encompassing "any infrastructure whose breach or data leakage could endanger

[10] "中华人民共和国保守国家秘密法 [Guarding State Secrets Law of the People's Republic of China]," *The State Council, The People's Republic of China*, Feb 27 2024, accessed Mar 28 2025, https://www.gov.cn/yaowen/liebiao/202402/content_6934648.htm

[11] "中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China]," *The State Council, The People's Republic of China*, Nov 7 2016, accessed Mar 28 2025, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

national security or the public interest."[12] This ambiguity makes it particularly difficult for foreign companies to determine whether their services or operations fall within the law's scope. Consequently, many international firms resort to self-censorship or overly cautious practices to avoid potential non-compliance. Additionally, the CL contains provisions obliging companies to assist and cooperate with China's national security apparatus during investigations. Such assistance could include turning over data to the law enforcement and security authorities. Non-compliance would bear legal consequences. These requirements have raised serious concerns among multinational enterprises and Western policymakers, particularly regarding the potential for Chinese authorities to demand access to data held on overseas service users—posing significant risks to the data rights of individuals and entities that may be of strategic interest to the Chinese state.

A key feature of the Cybersecurity Law (CL) is the establishment of a precedent for extraterritorial application in cybersecurity-related legislation. The CL stipulates that China's national security authorities may impose sanctions or freeze the assets of any foreign organisation, agency, or individual deemed to be engaging in activities that threaten the country's critical information infrastructure. This provision represents an effort to extend the People's Republic of China's concept of cyber sovereignty beyond its physical borders and serves as a deterrent to entities within China considering collaboration with foreign companies, due to the associated legal and political risks. In essence, the CCP underscores the imperative of maintaining the flow of information within China and firmly under Party control, thereby laying the foundation for further legislation aimed at restricting foreign access to information within the country.

In addition, the Cybersecurity Law (CL) includes provisions aimed at protecting individual privacy, requiring service providers not to leak, alter, or damage the personal information they collect. The language of these clauses closely mirrors that of Western

[12] "关键信息基础设施安全保护条例 [Regulations on Security Protection of Critical Information Infrastructure]," *The State Council, The People's Republic of China*, Aug 17 2021, accessed Mar 28 2025, https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

data protection legislation, albeit with an added emphasis on safeguarding national security. However, in practice, the enforcement of these provisions has made it increasingly difficult for entities to access data that could be classified as personal, regardless of the context or purpose. This restrictive approach laid the groundwork for more comprehensive regulation, culminating in the introduction of the Personal Information Protection Law (PIPL), developed by the SCNPC to further govern the handling and provision of personal data.

2.3.2 Data Security Law (DSL)

In its continued effort to retain data within its borders and restrict foreign access, the Standing Committee of the National People's Congress (SCNPC) passed the Data Security Law (DSL) in June 2021. The DSL explicitly prohibits internet operators and service providers operating in China from transferring data originating in the PRC to foreign judicial or law enforcement agencies without prior approval from the Chinese government. The law mandates that different levels of government establish a system for classifying and protecting data, with particular emphasis on evaluating the potential risks to national security in cases of data tampering, leakage, or damage.[13] The enactment of the DSL effectively erects another barrier between China and the global information ecosystem, as cyber operators within the country are legally forbidden from sharing data with external partners—further constraining information freedom within Chinese territory.

2.3.3 Personal Information Protection Law (PIPL)

The protection and control of personal data have been central to the legislative agenda of the Standing Committee of the National People's Congress (SCNPC). Building on earlier provisions included in the Cybersecurity Law (CL) and the Counter Espionage Law (CSL), the SCNPC enacted the Personal Information Protection Law

[13] "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," *The State Council, The People's Republic of China*, June 11 2021, accessed Mar 28 2025, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm

(PIPL) in August 2021, aiming to establish a comprehensive legal framework to regulate the circulation of personal data. The PIPL defines "personal information" broadly, encompassing all categories of data—recorded electronically or by other means—that could be used to identify natural persons. Owing to the law's vague and expansive definition, as well as the potential legal penalties for non-compliance, many companies have adopted restrictive practices in relation to data sharing. This has significantly hindered access to information for business and academic researchers, posing particular challenges to the business due diligence sector, as discussed elsewhere in this report.

While the PIPL emphasises the responsibility of network operators and service providers to handle personal information with due care and obtain the individual's consent, it reinforces the stringent restrictions on cross-border data transfers already established in the Cybersecurity Law (CL) and the Data Security Law (DSL). The PIPL grants China's cybersecurity authorities the power to publicly denounce and blacklist overseas organisations or individuals deemed to be engaging in activities that undermine national security. Once blacklisted, any requests for information transfer to these entities are explicitly prohibited, further limiting international data flows and reinforcing the government's control over personal information.[14]

Another concern on PIPL lies in its applicability to state organs of China. As researchers in Stanford University highlighted, "questions remain about the extent to which state organs will in fact be required to comply with personal information handler responsibilities, including requirements set forth in Chapter V [of PIPL] to appoint a personal information protection officer; conduct audits and impact assessments; report leaks and other risks; and establish compliance structures and publish social

[14] "中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China]," *The State Council, The People's Republic of China*, August 20 2021, accessed Mar 28 2025, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

responsibility reports under Article 58 [of PIPL]."[15] As PIPL has passed for a few years, it is essential to observe whether the Chinese government will improve governance on personal information from within.

2.3.4. Network Data Security Management Regulations (NDSMR)

The most recent legislative effort to expand the regime's control over information freedom is the introduction of the Network Data Security Management Regulation (NDSMR), issued by the State Council. The NDSMR builds upon provisions first outlined in the Personal Information Protection Law (PIPL), requiring network operators that process the personal data of over 10 million individuals to conduct annual risk assessments. These assessments must be made available for review by the Cyberspace Administration of China (CAC) or relevant branches of the national security apparatus. The regulation specifies that the assessments must evaluate the risks that data tampering, theft, or leakage could pose to national security.[16] In doing so, the NDSMR significantly reinforces the supervisory powers of cybersecurity and national security authorities over the operations of network operators and service providers. The regulation came into force in January 2025, and China observers are closely monitoring how its implementation may further erode information freedom in the country.

---

[15] Alexa Lee et al, "" DIGICHINA, Stanford University, Sep 15 2021, accessed Apr 2 2025, https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/#:~:text=Questions%20remain%20about%20the%20extent,report%20leaks%20and%20other%20risks

[16] "网络数据安全管理条例 [Network Data Security Management Regulation]," *The State Council, The People's Republic of China*, Sep 30 2024, accessed Mar 28 2025, https://www.gov.cn/zhengce/content/202409/content_6977766.htm ; "司法部、国家网信办负责人就《网络数据安全管理条例》答记者问 [Ministry of Justice and Cybersecurity Administration Answering Reporters' Questions Regarding 'Network Data Security Management Regulation']," *The State Council, The People's Republic of China*, Sep 30 2024, accessed Mar 28 2025, https://www.gov.cn/zhengce/202409/content_6977835.htm

3. CCP's current approaches to China's information environment

3.1 Why has the information environment been tightened?

Despite its long-standing restrictions on information freedom, the Chinese state has significantly intensified its control over cyberspace over the past decade, under the banner of defending "cyber sovereignty" and safeguarding "cybersecurity." This trend is primarily driven by the Chinese Communist Party's (CCP) heightened focus on national security and economic security.

3.1.1 National Security

At the core of China's increasingly restrictive information environment is the regime's emphasis on "national security," which is closely aligned with President Xi Jinping's broader campaign to consolidate the Chinese Communist Party's (CCP) power domestically. In practice, the CCP's concept of "national security" largely equates to "regime security." This interpretation goes far beyond conventional understandings of national security—such as safeguarding territorial integrity or countering terrorism—and instead encompasses the preservation of the Party's authority and ideological dominance. Since assuming power in 2012, President Xi has consistently underscored the importance of reinforcing CCP leadership. During his first appearance as President at the National People's Congress (NPC) in March 2013, he stressed the need to comprehensively strengthen the Party's leadership capacity.[17] Later that year, he delivered a speech reiterating that while economic development is essential, the control of ideology is "fundamental" to national security.[18] He warned that, without firm ideological oversight, the CCP's leadership risked being undermined by the infiltration of Western values and ideas.

From President Xi's perspective, national security remains a paramount priority—one that can only be secured through the continued strengthening of the CCP's

---

[17] Xi Jinping, "在十二届全国人大一次会议上的讲话 [Speech at the First Session of the Twelfth National People's Congress]," *The State Council, The People's Republic of China*, Mar 17 2013, accessed Mar 28 2025, https://www.gov.cn/ldhd/2013-03/17/content_2356344.htm

[18] Xi Jinping, "8.19 讲话全文：言论方面要敢抓敢管敢于亮剑 [8.19 speech full text: regarding speech, we should dare to grasp, dare to control, and dare to show the sword]," *China Digital Times*, Nov 4 2013, accessed Mar 28 2025, https://chinadigitaltimes.net/chinese/321001.html

authority. Ideological control serves as a central pillar in maintaining political stability. By consolidating its dominance over the flow of information, the CCP is able to effectively identify, manage, and suppress narratives that could pose a challenge to the authority of the state.

3.1.2 Economic Security

Economic security is another key driver behind China's increasingly restrictive information policies. In recent years, following allegations of forced labour in Xinjiang, China has been subjected to sanctions imposed by several Western countries. Products connected to Xinjiang's supply chains have been specifically targeted and, in some cases, banned outright.[19] This has had a notable economic impact, given the region's critical role in national manufacturing—accounting for nearly 90% of China's cotton and fine wool production.[20]

Additionally, rising geopolitical tensions—most notably the deteriorating relationship between the United States and China—have prompted the US to impose increasingly stringent restrictions on trade involving critical resources and entities linked to China's military.[21] Due to China's policy of military-civil fusion, in which military and civilian sectors are closely intertwined, many sensitive industries—such as defence-related manufacturing—are deeply embedded within the broader economy.[22] As a result, substantial segments of China's economic landscape are exposed to the risk of US sanctions and trade restrictions.

---

[19] "Against Their Will: The Situation in Xinjiang," *Bureau of International Labor Affairs, U.S. Department of Labor*, accessed Mar 28 2025, https://www.dol.gov/agencies/ilab/against-their-will-the-situation-in-xinjiang

[20] Ines Liu, "Investing in Xinjiang: Economy, Industry, Trade, and Investment Profile", *China Briefing*, accessed Mar 28 2025, https://www.china-briefing.com/doing-business-guide/china/where-to-invest/investing-in-xinjiang-economy-industry-trade-and-investment-profile

[21] Humeryra Pamuk, Alexandra Alper & Idrees Ali, "Trump bans U.S. investments in companies linked to Chinese military," *Reuters*, Nov 13 2020, accessed Mar 28 2025, https://www.reuters.com/article/usa-china-securities-idUSKBN27T1MD/

[22] "国务院办公厅关于推动国防科技工业军民融合深度发展的意见 [Opinion of the General Office of the State Council on Promoting the Development of Civil-Military Fusion in the Defence Science," *The State Council, The People's Republic of China*, December 4 2017, accessed Mar 28 2025, https://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm

By tightly controlling data and information flows, China seeks to mitigate the risks associated with international sanctions and to shield its economic activities, including those involving sanctioned entities. This strategy is viewed as essential to preserving China's economic resilience in the face of ongoing decoupling trends and sustained efforts by Western governments to restrict its access to critical technologies.

3.2 What are the approaches?

The contraction of information freedom in China can be understood as a strategic measure to safeguard both national and economic security. The following approaches illustrate how these objectives are pursued (see Figure 1 below):

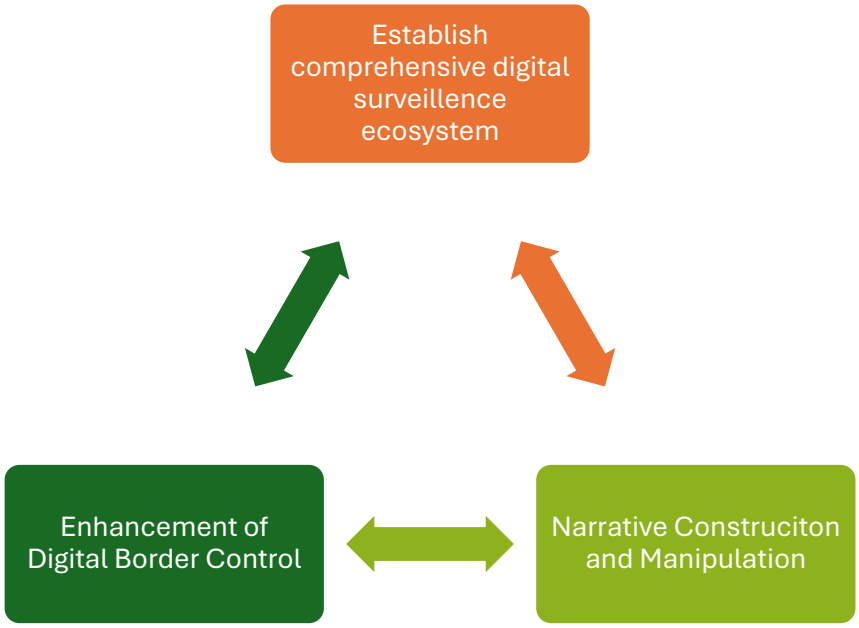

Figure 1. China's 3-prong Approach to restricting information freedom.

3.2.1 Establishment of Comprehensive Digital Surveillance

China has developed a highly sophisticated digital surveillance ecosystem that underpins its broader strategy of information control. Beyond its well-known "Skynet" surveillance network, the state has implemented a wide array of digital monitoring systems. [23] As detailed further in this report, China's surveillance apparatus encompasses virtually all online activities within its borders, including public forums, social media platforms, and private communications. While the presence of state surveillance is widely recognised, it also cultivates an environment of pervasive self-censorship—both among Chinese citizens and foreign nationals residing or working in the country.

3.2.2 Narrative Construction and Manipulation

In addition to its extensive surveillance apparatus, China actively shapes public opinion through the manipulation of media content and online discourse. State-run media outlets and domestic social platforms disseminate carefully curated narratives aligned with Party priorities, while coordinated campaigns are deployed to censor, suppress, or overwhelm dissenting voices. In effect, information manipulation occurs when political authorities enable disinformation campaigns and systematically eliminate diverse and pluralistic perspectives, including independent opinions and critical commentary. These efforts are often executed by criminalising and penalising individuals who share or produce critical information. Moreover, the state mobilises nationalist netizens to actively engage in online discussions, amplifying official narratives and crowding out contentious viewpoints—effectively neutralising public dissent in the digital sphere.

3.2.3 Enhancement of Digital Border Control

Digital border controls—most notably the "Great Firewall"—are central to China's strategy of restricting the flow of external information into the country. By blocking foreign platforms and tightly regulating data transmission, the government has

---

[23] Xinmei Shen, "Skynet, China's massive video surveillance network," *South China Morning Post*, Oct 4 2018, accessed Mar 28 2025, https://www.scmp.com/abacus/who-what/what/article/3028246/skynet-chinas-massive-video-surveillance-network

effectively isolated its domestic internet ecosystem, limiting exposure to external ideas and influences. Recent legislation, including the Data Security Law and the Personal Information Protection Law, further tightens restrictions on cross-border data flows, placing state control above transparency and international cooperation. Additionally, the application of espionage laws against foreign individuals or organisations serves as another tool of digital border enforcement. The transmission of information deemed to be “state secrets” from within China can constitute a criminal offence, even in cases involving foreign actors. This approach disrupts the internal information supply chain and severs the flow of information between China and the international community, thereby facilitating the state’s broader objectives of political propaganda and public opinion control.

4. Impacts on the Private Sector

Generally speaking, firms engaged in due diligence related to China are facing increasingly stringent limitations. By restricting access to corporate data and curtailing operational transparency, the Chinese government effectively shields key industries, state-owned enterprises, and politically sensitive projects from external scrutiny. This also hinders foreign entities from acquiring insights that could be used to question China's economic practices or support the imposition of international sanctions. This section outlines seven key issues illustrating how China's restrictive information environment has affected the private sector—particularly the due diligence industry.

4.1 Rapid growth of China's business intelligence and due diligence industry before the state crackdown

> *"Despite China's rapid economic growth, fraud has been a pervasive issue, with some companies falsifying documents and exaggerating financial performance when reporting to regulators and investors. This widespread problem highlights the need for due diligence, as our responsibility is to help clients avoid falling victim to fraud. By conducting thorough investigations, our company ensures our clients can make informed decisions and prevent financial losses."*
>
> *"M", an employee at a multinational due diligence firm, 8 December 2024.*

Prior to the regulatory crackdown on the sector, China's due diligence industry experienced rapid growth, driven by the increasing need to combat financial fraud. The issue gained prominence in 2011, when the total market value of Chinese companies delisting from the New York Stock Exchange—often as a result of fraudulent activity—

significantly surpassed that of new Chinese IPOs.[24] In response, domestic business intelligence consultancies such as Meritco, BDA, and B-Core emerged, while foreign firms including Control Risks, Kroll, and Mintz Group expanded their presence in the Chinese market. These consultancies primarily offered business intelligence and due diligence services to foreign clients seeking to invest in or operate within China. Due diligence proved vital for these clients, providing transparency and reducing the risk of fraud—thereby enabling more informed decision-making and helping to avoid engagement in opaque or unpredictable business environments.

"M," an employee at a multinational due diligence firm with 14 years of experience, remarked that "local knowledge is the key to effective due diligence." He explained that a deep understanding of the Chinese market, language, and business culture makes it significantly more difficult for companies to provide misleading information. This reliance on local expertise, he noted, is a key reason why many foreign companies seek professional due diligence support when operating in China. He further observed that during periods of high foreign direct investment (FDI) into China, "the demand for our due diligence services grew significantly."[25]

In addition to commercial considerations, the growing demand for due diligence services in China was also driven by the need to comply with international regulatory frameworks. Foreign governments enforce anti-bribery and anti-corruption laws that often apply extraterritorially to multinational companies conducting business in China. These regulations require firms to uphold global ethical standards and legal obligations, thereby reinforcing the importance of due diligence in identifying potential compliance risks. "M" explained, "The Foreign Corrupt Practices Act (FCPA) prohibits U.S. individuals and companies from offering, paying, or promising to pay money or anything of value to foreign officials to obtain or retain business. Multinational firms need to know whether individuals or companies pose any corruption risk. As a result, some clients

---

[24] "Hoaxes and Hijinks: China's Growing Due Diligence Industry," *Sixth Tone*, Mar 21 2022, accessed Mar 28 2025, https://www.sixthtone.com/news/1009930

[25] RIL interview with M (pseudonym), Online, Dec 2 2024.

have approached our company to conduct enhanced due diligence on specific subjects to ensure compliance with the Act."[26]

4.2 State crackdown on due diligence

> *"National security agencies, during the investigation of several cases, have discovered that many foreign institutions with complex backgrounds attempt to bypass China's laws, regulations, and oversight of major sensitive industries by concealing or downplaying their foreign ties. They exploit domestic consulting firms and other industries to steal national secrets and intelligence in critical areas. Some domestic consulting firms, lacking awareness of national security, frequently operate on the verge of legality in pursuit of economic gain."*
>
> *News report made by China Central Television, accusing Capvision of illegally gathering sensitive data, 9 May 2023*

Shortly after President Xi assumed office in 2012, Beijing had already begun targeting foreign due diligence professionals. However, such cases remained relatively limited in number during the early years of his presidency.

The most notable early case involved Peter Humphrey, a former Reuters correspondent and fraud investigator working for Western companies in China. In August 2013, Humphrey was detained and subjected to daily interrogations by the Public Security Bureau (PSB), followed by questioning from the Ministry of State Security.[27] His case was linked to a high-profile corruption scandal involving

[26] Ibid.
[27] Peter Humphrey, "China's new anti-spy law is just the beginning," *Politico*, May 24 2023, accessed Mar 28 2025, https://www.politico.eu/article/chinas-new-anti-spy-law-is-just-the-beginning/

GlaxoSmithKline (GSK), a British multinational pharmaceutical company operating in Mainland China.

In January 2013, an anonymous email alleging bribery at GlaxoSmithKline (GSK), along with a sex tape involving the company's China chief, Mark Reilly, surfaced—prompting GSK to hire Peter Humphrey's due diligence firm, ChinaWhys, to conduct an internal investigation. Humphrey delivered his findings in June 2013. Just one month later, Chinese authorities launched an official investigation into GSK China and detained four of its employees. Humphrey was subsequently arrested and accused of espionage, with authorities citing publicly available reports found on his computer and attempting to link him to intelligence-gathering activities—allegations he firmly denied. He was ultimately convicted of "illegally acquiring personal information" and sentenced to 30 months in prison, while his American wife and business partner, Yu Yingzeng, received a two-year sentence. Their firm, ChinaWhys, was forcibly shut down following their arrest. Both were released in 2015 and deported from China.

In an article published by *Politico*, Peter Humphrey claimed that many professionals in the due diligence industry fled China out of fear of arrest.[28] Following his detention, Chinese authorities issued warnings to other due diligence firms and imposed strict measures that severely curtailed their operations. After his release, former and prospective clients reached out to him in search of the services and support he had previously provided. When asked who could now deliver the same high standard of due diligence, Humphrey could only respond that no one could. His experience underscores the extent to which the due diligence industry has been constrained under President Xi's leadership.

[28] Peter Humphrey, "Foreign business community in China beware," *Politico*, Apr 5 2023, accessed Mar 28 2025, https://www.politico.eu/article/mintz-china-foreign-business-due-diligence/

> *"The biggest risk is that you tread on the toes of someone you investigate by discovering things they don't want to be known. And if they are connected to the Communist Party, they will then leverage their contacts to get you arrested."*
>
> Peter Humphrey, 5 April 2023.[29]

Humphrey's arrest marked the beginning of a broader state-led crackdown on foreign business consultancies, with further arrests and investigations following in subsequent years. In April 2023, Chinese police visited the Shanghai office of Bain & Company, a prominent American business consulting firm, and later questioned several of its employees.[30] In May 2023, authorities targeted another firm, Capvision, accusing it of failing to meet its counterintelligence obligations. Officials alleged that Capvision had hired well-connected experts to obtain sensitive information, thereby posing a threat to national security. State security officers raided the company's offices in several major cities, questioned staff, and seized materials. In response, Capvision pledged to strengthen its compliance with national security regulations and committed to supporting efforts to tighten oversight across the consulting industry.[31]

4.3 State Crackdown on Due Diligence Work about Xinjiang

China's relations with many foreign countries—particularly Western nations—have deteriorated in recent years. These heightened tensions have led to increased scrutiny on a range of issues, most notably human rights concerns in the Xinjiang

[29] Ibid.
[30] Ibid.
[31] Kelly Ng, "Capvision: China raids another consultancy in anti-spy crackdown," *BBC News*, May 9 2023, accessed Mar 28 2025, https://www.bbc.co.uk/news/world-asia-china-65530082

Uyghur Autonomous Region (XUAR). Alarmed by reports of forced labour and other alleged human rights violations, Western governments have intensified their efforts to hold Chinese entities accountable through diplomatic measures, trade restrictions, and sanctions.

Western democracies, particularly the United States, have introduced stricter laws and regulations to combat global forced labour, especially within the broader context of trade tensions with China. In December 2021, the U.S. Congress passed the Uyghur Forced Labour Prevention Act (UFLPA), which was subsequently signed into law by President Joe Biden. The legislation aims to prevent goods produced using forced labour in the Xinjiang Uyghur Autonomous Region (XUAR) from entering U.S. markets. It establishes a “rebuttable presumption” that all goods originating from Xinjiang are produced with forced labour unless importers can provide clear and convincing evidence to the contrary.

Media outlets and human rights organisations have increasingly raised concerns and issued criticisms regarding businesses that source raw materials from the Xinjiang Uyghur Autonomous Region (XUAR) or are linked to the use of forced labour. As a result, multinational companies are facing mounting pressure to ensure that their supply chains are free from any association with forced labour originating in the XUAR.

In an effort to avoid sourcing from the Xinjiang Uyghur Autonomous Region (XUAR), multinational corporations operating in China have strengthened their due diligence and supply chain tracing mechanisms. According to M, multinational firms are unable to access the XUAR directly to conduct due diligence or verify the origin of raw materials. As a result, these companies must rely on specialised supply chain due diligence services to assess associated risks, ensure compliance with international regulations, and mitigate potential legal liabilities or reputational harm.

M noted that due diligence consultancies saw an increase in requests for supply chain tracing services related to the Xinjiang Uyghur Autonomous Region (XUAR), particularly following the enactment of the Uyghur Forced Labour Prevention Act

(UFLPA). However, this rising demand also led to increased scrutiny and a broader crackdown by Chinese authorities on consultancies conducting due diligence work connected to XUAR-related investigations.

In March 2021, Chinese police raided the Beijing office of Mintz Group, a multinational due diligence firm specialising in fact-gathering and internal investigations. Authorities detained five local staff members during the operation. The raid sent shockwaves through the Chinese business community and raised concerns among due diligence consultancies, including those based in Hong Kong. According to a Reuters report, Mintz Group had conducted corporate due diligence investigations into the possible use of forced labour within supply chains linked to the Xinjiang Uyghur Autonomous Region (XUAR).[32] However, it remains unclear whether the raid was directly related to this work, as neither Mintz Group nor the Chinese authorities have disclosed the details of the investigation.

Although Mintz Group maintained that it had operated legally in China, the company was subjected to severe penalties for its activities. On 6 July 2024, the Beijing Municipal Bureau of Statistics issued a notice stating that Mintz Group had been fined approximately USD 1.5 million (around GBP 1.23 million) for conducting "unauthorised statistical work." According to the bureau, the company carried out 37 unauthorised foreign-related statistical investigations between March 2019 and July 2022. As part of the penalty, authorities confiscated RMB 5.34 million (approximately GBP 589,000) in what was described as "illegal proceeds" and imposed a matching fine. The notice did not disclose whether the five detained Chinese staff members were prosecuted, nor did it provide supporting evidence for the allegations. In March 2025, Mintz Group announced that its five Chinese employees had been released after two years in

[32] James Pomfret & Engen Tham, "Exclusive: US consultancy Mintz's executives leave Hong Kong after China raid," *Reuters*, May 19 2023, accessed Mar 28 2025, https://www.reuters.com/world/china/us-consultancy-mintzs-executives-leave-hong-kong-after-china-raid-sources-2023-05-19/

detention, although the company did not disclose the reasons behind their initial detention.[33]

4.4 Exit bans on executives of due diligence consultancies

Chinese authorities have also imposed exit bans on senior executives within the due diligence industry. In September 2023, an exit ban was placed on Michael Chan, a Hong Kong-based Managing Director at Kroll. Chan was reportedly assisting with an investigation linked to a case from several years prior.[34] According to Ben (pseudonym), a due diligence analyst at Kroll with two years of experience, the exit ban came as a shock to staff, especially given that Chan was neither prosecuted nor formally arrested.[35] Ben noted that the company shared limited details about the situation, preferring to handle the matter discreetly and maintain a low profile.

Prior to the restrictions on Chan, a senior banker at Nomura Holdings Inc. was also prohibited from leaving China in relation to an ongoing investigation involving a high-profile dealmaker. Charles Wang Zhonghe, Chair of Investment Banking for China at Nomura's Hong Kong division, was not detained but remains subject to exit restrictions. These cases underscore China's increasingly hostile stance toward foreign businesses, particularly those operating in sensitive sectors such as due diligence and financial services.

4.5 Informal warnings

In addition to the formal crackdown on the industry, Chinese authorities have reportedly employed informal methods to exert pressure on due diligence firms

---

[33] Antoni Slodkowski & Liz Lee, "China frees Mintz staff in move to soothe foreign sentiment," *Reuters*, Mar 25 2025, accessed Mar 28 2025, https://www.reuters.com/world/china/china-releases-mintz-employees-after-two-year-detention-company-says-2025-03-25/

[34] Kari Soo Lindberg, "China Bars Executive at US Firm From Leaving Mainland, WSJ Says," *Bloomberg UK*, Sep 29 2023, accessed Mar 28 2025, https://www.bloomberg.com/news/articles/2023-09-29/china-bars-executive-at-us-firm-from-leaving-mainland-wsj-says

[35] RIL interview with Ben (pseudonym), Online, Nov 29 2024.

operating in Mainland China. According to two senior executives from international due diligence firms with extensive experience in the country, Chinese security officials have periodically convened private meetings in recent years to issue explicit warnings about restricted areas for corporate investigations—most notably, Xinjiang.[36] These informal cautions serve as a deterrent, discouraging due diligence consultancies from pursuing lines of inquiry that the Chinese government considers politically sensitive.

4.6 Chilling effects on the due diligence sector

The raids on due diligence consultancies in Mainland China have prompted several firms to close their offices in Hong Kong and, in some cases, evacuate senior executives. Since the enactment of the Hong Kong National Security Law (HKNSL) in July 2020, due diligence activities involving Chinese individuals or entities can be deemed politically sensitive by national security authorities in Hong Kong. Following the March 2023 raid on its Beijing office by Chinese police, some Hong Kong-based staff of Mintz Group relocated to Singapore, reflecting a broader trend of firms seeking safer operational environments in the region.[37]

In addition, the crackdown on the due diligence industry in Mainland China has created a chilling effect, prompting consultancies to adopt a more cautious approach in handling their cases. Ben explained that his company had readjusted its internal policies to become more risk-averse. He noted that the Hong Kong team had ceased conducting due diligence related to politically sensitive topics in Mainland China—such as Xinjiang, military-civil fusion, and state-owned enterprises.[38] Any sensitive cases received in Hong Kong are now referred to colleagues in Singapore in order to "avoid any legal trouble" following the enactment of the Safeguarding National Security Ordinance (SNSO), also known as the domestic legislation pursuant to Article 23 of Hong Kong's Basic Law. Ben highlighted that the SNSO provides only vague definitions for offences

[36] Pomfret & Tham, "US consultancy Mintz's executives leave Hong Kong."
[37] Ibid.
[38] Ben, interview.

such as “theft of state secrets” and “espionage,” and expressed concern that the broad scope of these charges has further increased pressure on the due diligence industry.[39]

Furthermore, Ben noted that his company had reinforced its data security protocols, advising senior executives travelling to Hong Kong and Mainland China from other locations to use burner phones and refrain from bringing their regular work phones or laptops.[40] These precautions reflect growing concerns over surveillance and data interception. Similar practices have been reported elsewhere. In November 2023, the *Financial Times* reported that major audit and consulting firms—including Deloitte, KPMG, and McKinsey—had also advised their staff to use burner phones when visiting Hong Kong, citing data security concerns.[41]

“M” also noted that his company had adopted a more cautious approach when handling sensitive due diligence requests. He explained that no authorities had clearly defined where the “red lines” lay, leaving professionals in the industry operating in a climate of uncertainty. As a result, all potentially sensitive requests are now reviewed by the company’s legal and compliance departments to assess whether they pose any risk of violating national security laws. If there is any doubt, the company either declines the assignment or refers the request to colleagues based outside Hong Kong.[42]

4.7 Official Firewalls Obstructing Due Diligence

Since 2023, there have been growing reports indicating that China has used its internet firewall to block foreign researchers’ access to Chinese databases when accessed via offshore IP addresses, thereby impeding the work of overseas and Hong Kong-based due diligence professionals. As reported by *Hong Kong Free Press* (HKFP), several major Chinese corporate database platforms—including Tianyancha

[39] Ibid.
[40] Ibid.
[41] Slodkowski & Lee, “China frees Mintz staff.”
[42] M, interview.

and Qichacha—began restricting offshore access from March 2023.[43] HKFP's tests also revealed that numerous local Chinese government websites had become inaccessible from locations such as Hong Kong, Canada, the United States, the United Kingdom, and Australia. Websites belonging to municipal governments in provinces including Guizhou, Hebei, Fujian, and Shandong were among those found to be blocking foreign access.

An article published by *The China Project*, a New York-based China-focused news platform, on 6 July 2024, revealed further restrictions affecting access to Chinese data platforms. Since April 2023, Qichacha has required users to provide a Chinese phone number for authentication before access is granted. Overseas users have also reported losing access to Wind Information, one of China's leading financial data providers.[44] Similarly, Tianyancha now restricts access exclusively to users with IP addresses located within mainland China.

In addition to corporate information databases, Chinese authorities appear to have restricted foreign access to official government databases. *China Judgements Online*, an official platform providing access to legal records, now requires users to authenticate using a Chinese phone number. At the time of writing, the authors attempted to log in using a foreign phone number but were denied access. In effect, this means that foreign researchers without a Chinese phone number are unable to access the database. In many instances, local and overseas desk researchers have to provide a lot of private data for account registration and verification. These processes enable the state authorities to identify users' personal information, and then locate what they

---

[43] "Advisory firms on alert after China raids and arrests, as experts say data crackdown will hinder int'l investment," *Hong Kong Free Press*, May 15 2023, accessed Mar 28 2025, https://hongkongfp.com/2023/05/15/advisory-firms-on-alert-after-china-raids-and-arrests-as-experts-say-data-crackdown-will-hinder-intl-investment/

[44] Eduardo Jaramillo & Yi Liu,"Cut off from China's data and info, overseas academics, analysts get crafty," *The China Project*, July 6 2023, accessed Mar 28 2025, https://thechinaproject.com/2023/07/06/cut-off-from-chinas-data-and-info-overseas-academics-analysts-get-crafty/

search, browse and even their source of funds. These restrictive measures further limit transparency and the availability of legal information to external audiences.

Both M and Ben emphasised that access to Chinese corporate database platforms is essential to their due diligence work. These platforms provide detailed and specific information, including bankruptcy records, regulatory filings, and legal documentation within Mainland China.[45] They noted that such data is often not available through foreign corporate intelligence platforms such as Lexis Diligence or World-Check, making access to Chinese databases indispensable for conducting comprehensive risk assessments and corporate investigations.

China's firewall restrictions on database access have made conducting due diligence significantly more difficult. As a result, analysts have been forced to adopt alternative methods to retrieve essential information. An article published by *The China Project* outlined two commonly used workarounds. One approach involves the use of virtual private networks (VPNs) to simulate a Chinese IP address—a technique similar to that used by Chinese travellers abroad to access streaming platforms like iQiyi, which are otherwise unavailable outside China. Another method involves purchasing restricted data from vendors on Chinese e-commerce platforms such as Taobao. However, this requires researchers to be proficient in Chinese and familiar with the platform's distinctive user interface.[46] Both Ben and M confirmed that their companies employ such methods to access key databases, though they declined to elaborate further on their research techniques, citing internal confidentiality policies.[47]

Accessing and obtaining critical information from official Chinese databases and other restricted sources presents considerable challenges for foreign-based due diligence consultancies. Both Ben and M stated that although they were able to access some official databases using virtual private networks (VPNs), they had experienced repeated disruptions—suggesting that Chinese authorities may have interfered with

[45] Ben, interview.
[46] Ibid.
[47] Ben, interview.

VPN connections to hinder access.[48] Ben further explained the difficulties involved in acquiring restricted data, noting that while some information can be purchased through vendors on Chinese e-commerce platforms such as Taobao, obtaining corporate data on sensitive state-owned enterprises is nearly impossible. He emphasised that selling such information to foreign-based due diligence consultancies carries significant risks, as Chinese authorities may interpret such activities as acts of espionage.[49]

"Once, I approached a vendor who had previously worked with us, asking for the legal records of a Chinese state-owned aerospace and military manufacturer. The vendor immediately blocked me and never responded again. I suspect he considered the transaction too risky, fearing it could result in charges related to national security," Ben said.[50] He added that in the absence of access to such restricted data, firms are often forced to complete due diligence investigations with only limited information, significantly undermining the depth and reliability of their assessments.

[48] M, interview.
[49] Ben, interview.
[50] Ibid.

5. Impacts on Civil Society Stakeholders

China's information controls disproportionately target groups with significant social influence and strong links to foreign actors. These organisations are perceived by the state as potential conduits for external ideas or interference and are therefore subjected to heightened scrutiny and restrictions. Non-governmental organisations (NGOs) and advocacy groups, in particular, are viewed as threats to the regime's authority due to their capacity to mobilise grassroots movements and draw attention to human rights abuses. Civil society actors with international connections are especially targeted, as they are seen as potential channels for foreign influence and ideological infiltration.

Furthermore, small-scale journalism and foreign press are key targets of China's information control efforts. Domestic journalists operate under strict censorship, while foreign correspondents frequently face surveillance, harassment, or even expulsion. These measures are designed to ensure that individuals within China are exposed only to state-approved content, while preventing the disclosure of sensitive information that the Chinese Communist Party (CCP) seeks to suppress.

Researchers and academics working on politically sensitive topics—such as governance, international relations, or technology—also face considerable restrictions. Academic exchanges with foreign institutions are closely monitored, with the aim of preventing the dissemination of information that challenges official narratives or reveals strategic vulnerabilities. These constraints have a chilling effect on academic freedom and limit opportunities for open, collaborative research.

5.1 Impact on Civil Society

For decades, civil society in China has operated under strict state surveillance and control. All non-governmental organisations (NGOs) are required to register and obtain official approval from the Ministry of Civil Affairs to operate legally—yet the majority of applications are unsuccessful. In 2013, a leaked internal document titled *The Communiqué on the Current State of the Ideological Sphere* (关于当前意识形态领域情

况的通报), commonly known as "Document Number Nine," revealed the ideological stance of the Chinese Communist Party (CCP) toward civil society. The document explicitly labelled "civil society" as a Western concept that threatens to undermine the Party's leadership at the grassroots level. Since its release, Chinese political authorities have adopted an increasingly hostile posture towards civil society organisations, viewing them as instruments of foreign influence and potential sources of dissent. [51]

That said, rather than relying solely on the enforcement of criminal law, Chinese authorities often incapacitate NGOs and community organisers through the use of the highly developed Great Firewall system. This infrastructure enables the removal of online content and the shadow banning of social media accounts, effectively curtailing digital visibility and engagement. Shi, a former Chinese community organiser, acknowledged that these measures severely disrupted her work by marginalising her organisation's presence in cyberspace.[52] She had previously used her Weibo account—followed by over 100,000 users—to communicate with the public and share information about her organisation's activities. When her account was suddenly banned without explanation, she described feeling as though her connection to the public had been abruptly severed.

One of the most frustrating challenges for NGOs and community organisers is the lack of consistency in censorship enforcement. Content that was once tolerated by the authorities may suddenly become prohibited without any prior notice or explanation. As revealed by a former Chinese internet censor, those responsible for content moderation are rarely given clear criteria; instead, they act based on directive guidance received from higher authorities.[53] Given that such guidance is subject to frequent revision and varying interpretations among different censors, it becomes virtually impossible to identify a clear boundary between permissible and prohibited content.

---

[51] "高瑜泄密—九号文件 [Gaoyu leaks – Document Number Nine]," *China Aid*, Apr 17 2025, accessed Mar 28 2025, https://www.chinaaid.net/2015/04/blog-post_19.html

[52] RIL interview with Shi (pseudonym), Online, Nov 27 2024.

[53] 王晓 [Wang Xiao], "中国 Z 世代审核员：生存吃饭最重要 [China's Gen Z Internet Censor: Surviving is the Most Important]," *Mang Mang*, Oct 14 2024, accessed Mar 28 2025, https://read.mangmang.run/p/z

This uncertainty fosters a climate of fear and self-censorship, further restricting civil society's ability to operate effectively.

In addition to public content on social media, NGOs and community organisers are acutely aware that their private communications are also subject to state surveillance. Guang, a diasporic Chinese LGBTQ activist who left China in 2023, recounted that it was common for police to pre-emptively appear at private gatherings—even when these were organised discreetly among trusted friends via private chats on WeChat. According to Guang, this pattern strongly suggested that their communications were being monitored, underscoring the extent to which surveillance permeates both public and private spheres of civil society activity in China.[54]

Peter, a veteran employee of an international non-governmental organisation (INGO) who was posted to China in the early 2000s, also shared a similar experience. Several years ago, he held regular meetings with a local government official. On one occasion, the official confronted him with materials that had only been shared within his organisation's internal group chat.[55] While not definitively proven, it is strongly suspected that the information was obtained through digital surveillance by the authorities.

Traditionally, many individuals within Chinese civil society have relied on virtual private networks (VPNs) to access state-banned websites, obtain censored information, and avoid state surveillance. However, following the implementation of the Cybersecurity Law in 2017—which requires all VPN service providers operating in China to obtain government approval—authorities have significantly tightened control over VPN usage. In the immediate aftermath of the legislation, more than 60 VPN providers were effectively removed from the market.[56] While a limited number of VPN services remain accessible, both Guang and Shi noted the growing presence of so-called "phishing VPNs" in China—tools that appear functional but are suspected of enabling the authorities to monitor users' online activities.

---

[54] RIL interview with Guang (pseudonym), Online, Nov 27 2024.
[55] RIL interview with Peter (pseudonym), Online, Dec 3 2024.
[56] "Apple 'pulls 60 VPNs from China App Store'," *BBC News*, July 31 2017, accessed Mar 28 2025, https://www.bbc.co.uk/news/technology-40772375

Unclear red lines, pervasive digital surveillance, and the declining availability of accessible and reliable VPNs have created mounting challenges for civil society in China. In response to this increasingly repressive environment, community organisers often resort to self-censorship—even in private conversations—as a precaution against potential state monitoring and retaliation.

> *"There is no safe place [...]. The state knows everything you speak."*
>
> *Guang*

Foreign NGOs face even greater challenges when operating in cyberspace and navigating administrative procedures in China. As Peter noted, in addition to persistent monitoring by local authorities, foreign NGOs are often burdened with complex and inconsistent bureaucratic requirements. Different government departments frequently provide conflicting information about the necessary paperwork, resulting in confusion and delays. Even when clear guidelines exist, individual officials may interpret them differently, imposing varying and sometimes contradictory demands—none of which are guaranteed to be correct.

To manage these administrative burdens, many foreign NGOs previously collaborated with local NGOs to reduce costs and streamline operations. However, following the implementation of the Foreign NGO Law in 2017, Peter observed a deliberate shift by authorities to exclude foreign NGOs from China's civil society landscape. Many local organisations that had once been willing partners became reluctant to collaborate, fearing potential political repercussions. As a result, numerous foreign NGOs have either ceased their operations in China entirely or significantly scaled back their presence.

There is no official data detailing how many foreign NGOs have withdrawn from China or how many have had their operations adversely affected by the law. However, according to information available on the Ministry of Public Security's website, as of March 2025, only 787 foreign NGOs were officially registered in China. Notably, nearly

half of these are industry or trade-promotion associations, which do not align with most people's intuitive understanding of non-governmental organisations.[57] Furthermore, of the 787 registered NGOs, over one hundred are listed as "de-registered," indicating a significant level of attrition within the sector.

5.2 Impact on Journalists

Since assuming power in 2012, President Xi Jinping has repeatedly underscored the importance of state control over journalism. In *Document Number Nine*, which outlines the so-called "seven wrong thoughts" (七条错误思潮), "freedom of the press" is labelled a Western concept that seeks to "oppose the leadership of the ruling party" by "infiltrating the country's ideology." During the 19th collective study session of the Chinese Communist Party (CCP) Politburo in 2019, Xi explicitly linked media oversight to the safeguarding of cybersecurity—framing journalism as a critical component of national security.[58] As emphasised by Karen, a former journalist who worked for three different media outlets in China over the past decade, journalists must avoid being perceived as promoting "wrong thoughts," as doing so risks severe professional and political consequences.[59]

> *"The golden rule to survive is not to publish anything that may go against the official narratives, if not actively echoing them."*
>
> *Karen*

[57] Foreign NGO Portal [境外非政府组织办事服务平台], accessed Mar 28 2025, https://ngo.mps.gov.cn/ngo/portal/toInfogs.do?p_type=1
[58] "习近平论新闻舆论工作 [Xi Jinping on News and Public Opinion Work]," *Wenming*, Dec 31 2023, accessed Mar 28 2025, http://www.wenming.cn/sxll/lszb/202112/t20211225_6274472.shtml
[59] RIL interview with Karen (pseudonym), Online, Dec 2 2024.

Foreign journalists in China often struggle to discern the boundary between permitted and prohibited topics. Jason, a foreign correspondent assigned to China in 2022, recounted an incident in which he sought to cover an environmental protection initiative in Beijing. Initially, local authorities approved the story. However, just a week later, he was informed—without explanation—that the topic could no longer be pursued. Such unpredictability reflects the opaque and shifting nature of media restrictions in China, leaving foreign journalists operating in a constant state of uncertainty.[60]

One of the consequences of stringent state control over the media is a widespread reluctance among individuals in China to speak with journalists, even under the condition of anonymity. As Jason observed with growing frustration, most people either declined or ignored his interview requests outright. In the rare instances where potential interviewees responded without an immediate refusal, they often asked—cautiously—whether the interview had been approved by the authorities. Jason estimated that, out of every hundred invitations, only two or three individuals would agree to be interviewed, and several of those would later express regret and request that their contributions not be published. As a result, verifying or cross-checking the accuracy of information has become an increasingly difficult task for journalists working in China.

Compounding these challenges is China's Great Firewall, which enables the rapid deletion of online content, creating further obstacles for journalists conducting research. Katherine, a foreign journalist stationed in China since 2018, described her work as "very challenging."[61] She frequently found herself struggling with scattered and incomplete information, and noted the absence of a reliable platform for accessing trustworthy sources. Given that online content in China can disappear without warning, Katherine explained that much of her time was spent indiscriminately backing up any material that might prove useful in the future—even content that seemed relatively benign—since no one can predict when it might be reclassified as sensitive.

---

[60] RIL interview with Jason (pseudonym), Online, Dec 1 2024.
[61] RIL interview with Katherine (pseudonym), United Kingdom, Nov 30 2024.

> *"After all, journalism in China often feels like walking in a mist."*
>
> *Katherine*

Compared to their local counterparts, foreign journalists in China face even greater challenges and hostility. In addition to intensive surveillance by the authorities, many report feeling unwelcome among the general public, further complicating their efforts to gather information. During the White Paper Movement in 2022, Jason's colleague attempted to cover the protests. Initially, he assumed that the demonstrators—perceived as more liberal-minded—would be receptive to foreign media. However, this assumption proved false. As a result, he was forced to conceal his identity as a journalist throughout the movement in order to complete his reporting. Katherine also shared her experience of being reported to local authorities after a failed attempt to contact a source for an interview, highlighting the heightened risks and mistrust foreign journalists often face on the ground.

> *"Rather than being hated, we are distrusted and feared in China (by the people). It is understandable, as it may already be a trouble for them to be in contact with us."*
>
> *Katherine*

Although state control over the media has long been stringent, the degree of enforcement varies over time, and the vague nature of censorship "red lines" often leads to confusion. It is widely acknowledged that certain politically sensitive dates—such as 4 June, which marks the anniversary of the 1989 Tiananmen Crackdown—trigger heightened surveillance. During such periods, journalists, particularly foreign correspondents, are closely monitored by authorities and often warned "not to do anything foolish." In some cases, they have even reported being unable to access the

internet. However, outside these politically sensitive windows, restrictions are generally more relaxed, allowing slightly more room for journalistic activity—albeit still within tight state-imposed limits.

5.3 On Academics

> *"We are facing a collective amnesia brought by the deliberate concealment of truth by the CCP. Thus, our mission to preserve memory becomes all the more crucial."*
>
> *Guo*[62]

Professor Guo Jian is the translator of *Tombstone*, authored by Yang Jisheng—one of the most comprehensive accounts of the Great Famine during Mao's era. Guo is also a founding contributor to the *Modern Chinese Political Campaigns Database*, which has archived more than thirty thousand historical records covering key political episodes, including the Land Reform to State–Private Partnership period (1949–1956), the Great Leap Forward and Great Famine (1958–1962), the Anti-Rightist Campaign, and the Cultural Revolution. These are chapters of Chinese history that the ruling elite are actively seeking to erase, and those involved in preserving such records are often targeted for challenging the regime's official historical narrative.

Guo believes that academic freedom in China has always been significantly constrained. Even during the relatively more permissive 1980s, the government launched campaigns to eradicate so-called "spiritual pollution" in academia. Historical research, in particular, has long been a sensitive and heavily restricted area under Communist rule. These constraints worsened in the aftermath of the Tiananmen

[62] RIL interview with Prof. Guo Jian, Online, Dec 1 2025.

Crackdown in 1989 and have reached new depths since Xi Jinping came to power, marking a further deterioration in the academic climate.

One of the most commonly used methods by the Chinese Communist Party (CCP) to suppress academic freedom is through the intimidation of scholars via routine, informal meetings with national security personnel—often euphemistically referred to as an "invitation for tea." During these encounters, academics are "reminded" not to publish content that could be deemed harmful to the regime's legitimacy.[63] In more overt cases, authorities have detained and interrogated overseas-based academics during visits to the People's Republic of China, further reinforcing the atmosphere of fear and self-censorship among scholars engaging with politically sensitive topics.

A notable example of the CCP's suppression of academic inquiry is the arrest of Professor Song Yongyi, a member of Guo Jian's editorial team, in 1999. Song was detained by China's national security apparatus upon returning to the country to collect historical materials related to the Cultural Revolution for a research project that would later contribute to the *Historical Dictionary of the Chinese Cultural Revolution* and the *Cultural Revolution Archive*. According to Guo, Song had only collected publicly available materials, such as speeches by CCP leaders and local newspapers sourced from private collectors. The arrest sparked widespread international condemnation, eventually compelling the Chinese government to acknowledge its mistake and release him.[64] Nevertheless, the authorities seized the opportunity to issue a stark warning to Song, cautioning him against continuing research that could expose the harsh realities of the Cultural Revolution—realities that implicate the CCP in widespread human suffering and threaten the regime's historical legitimacy.

---

[63] Yuwen Wu, "Tea? Reining in dissent the Chinese way," *BBC News*, Jan 15 2013, accessed Mar 28 2025, https://www.bbc.com/news/world-asia-china-21027416.amp

[64] Erik Eckholm, "China's Arrest Of Historian Based in U.S. Stirs Protests," *The New York Times*, Dec 31 1999, accessed Mar 29 2025, https://www.nytimes.com/1999/12/31/world/china-s-arrest-of-historian-based-in-us-stirs-protests.html

> *"Our books can only be published in Hong Kong or overseas. People in the PRC cannot even access our online Cultural Revolution database."*
>
> *Guo*

Before the rapid development of the internet and artificial intelligence, the Chinese government relied heavily on human resources to monitor and control academic activity. However, as cyberspace has evolved, so too have the tools available to the ruling elite for surveilling and suppressing individuals perceived as threats to the regime. For historians such as Guo, the ideal approach to conducting historical research involves physical presence in the PRC, allowing direct access to primary sources and archival materials. Yet, for many scholars, it became evident early on that such access was not feasible due to political and security risks. As a result, academics increasingly turned to online resources to conduct their research remotely.

However, as China tightened its grip on information flow within its borders, academics found it increasingly difficult to access search engines and historical databases in the PRC—even when using VPNs to bypass the Great Firewall. These restrictions have effectively severed the exchange of knowledge between China and the rest of the world. Ironically, many Chinese scholars have come to realise that conducting research abroad is now comparatively less challenging than doing so within their own country, underscoring the growing disconnect between China's academic community and global scholarship.

> *"What I truly worry about is whether our effort to uphold historical tradition, preserve public historical records, and independent research can overcome the regime's propaganda offensive that rewrites and whitewashes history. Together with the return of Mao worship and Lying Flatism (躺平主義), I am not optimistic."*[65]
>
> *Guo*

While Guo firmly believes that the official archives preserved by the Chinese government will eventually come to light, he remains deeply concerned about the current trajectory under Xi Jinping's leadership. In particular, he is alarmed by the regime's concerted efforts to reshape historical narratives to serve its political interests and to systematically erase collective memory from public consciousness. As a historian who has translated critical works and helped build databases that expose truths the Communist regime seeks to suppress, Guo shares the concerns of many academics in this field—especially regarding the risks to their personal safety and the safety of their families in China. Despite ongoing attempts by the state to obscure history and intimidate those who seek to uncover it, independent historians like Guo persist in their mission to preserve historical truth. As he puts it, these individuals are not necessarily conventional scholars, but rather people who see the act of preserving history as a moral obligation.

Although Guo remains pessimistic about the future of academic and information freedom within the Chinese sphere, he emphasises the importance of continued efforts

---

[65] While "Lying Flatism" initially referred to the trend of Chinese individuals choosing to disengage from work-centric lifestyles and accept lower living standards, in this context, it primarily describes a broader societal attitude—where individuals focus solely on their personal well-being and refrain from voicing criticism of the regime.

to preserve history as a form of resistance. When asked what can be done to mitigate the ongoing deterioration of academic freedom, Guo underscores the vital role of documenting and safeguarding historical truth. He urges individuals abroad to appreciate and make full use of the environments in which academic freedom is protected by institutions, and to persist in the work of historical preservation, ensuring that suppressed narratives are not lost to time.

6. Upcoming Challenges for Information Freedom in China

6.1 External Factors: Geopolitical Uncertainty and Transnational Surveillance

China's leadership confronts a volatile geopolitical environment that is prompting increasingly strict information control. Heightened tensions with Western powers and global instability have reinforced Beijing's belief that unrestricted information can threaten regime narratives. Analysts observe that Chinese authorities are progressively limiting data sharing and public information due to geopolitical pressures – they worry that online information could be weaponised to undermine policies or hinder development.[66] As discussed above, for instance, China's revised counter-espionage law in 2023 broadly prohibits transferring any data or documents related to national security, casting an extremely wide net over what qualifies as "state secrets".[67] This reflects Beijing's growing sensitivity to foreign scrutiny amidst uncertainty, as even openly available economic or academic data may be perceived as potential ammunition for rival states. Consequently, there is a diminishing space for factual reporting and research, with officials curating a narrative insulated from external criticism. Beijing's objective is to pre-empt perceived hostile influence by rigorously controlling the information ecosystem available to both domestic and foreign audiences.

At the same time, the CCP has expanded its surveillance and intimidation of citizens beyond its borders, targeting the overseas Chinese diaspora. Reports indicate that Chinese security agencies monitor and harass dissidents and expatriate communities abroad as part of "transnational repression".[68] The government closely

---

[66] Kai von Carnap, "The increasing challenge of obtaining information from Xi's China," Merics, Feb 15 2024, accessed Mar 28 2025, https://merics.org/en/report/increasing-challenge-obtaining-information-xis-china#:~:text=,to%20risks%20of%20information%20disappearing

[67] Thomas Shrimpton, "Beijing Expands Counter-Espionage Law to Crack Down on Foreign Access To Chinese Information," *Foreign Military Studies Office*, June 1 2023, accessed Mar 28 2025, https://fmso.tradoc.army.mil/2023/beijing-expands-counter-espionage-law-to-crack-down-on-foreign-access-to-chinese-information/#:~:text=In%20April%202023%20Chinese%20lawmakers,Beijing%20has%20detained%20dozens%20of

[68] "New Data: Mass Incidents Mark Dramatic Year of Transnational Repression, as 23 Governments Silence Exiles," *Freedom House*, Feb 6 2025, accessed Mar 28 2025,

monitors pro-democracy students, Uyghur and Tibetan activists, and other critics overseas by leveraging student associations, diaspora organisations, and even clandestine "overseas police service stations." Human Rights Watch has documented instances where Chinese police visited or threatened family members of Chinese students in Western countries to pressure those students into silence.[69] In one verified incident, authorities in China warned a student studying in Australia of possible prison time after he posted anonymous criticism of the government on Twitter, demonstrating that distance offers little protection from Beijing's reach.[70] Many Chinese abroad are acutely aware that their activities are being monitored; this creates a chilling effect in which individuals self-censor to avoid endangering themselves or their families.[71] Overall, growing geopolitical friction has fuelled Beijing's justification for such transnational surveillance, framing dissenting diaspora voices as "external threats." This external pressure translates into a significant challenge for information freedom, as even beyond China's borders, the flow of uncensored information and open discourse is stifled by fear of reprisal.

6.2 Internal Factors: Tightening Control Amid Economic Instability

Domestic pressures are also driving stricter state control over information and society. After decades of rapid growth, China's economy is facing headwinds – from slowing GDP and high youth unemployment to a property market crisis – which raise the spectre of social instability. The government's response has been to intensify censorship and propaganda to maintain public confidence and quell potential unrest.

---

https://freedomhouse.org/article/new-data-mass-incidents-mark-dramatic-year-transnational-repression-23-governments-silence#:~:text=Transnational%20repression%E2%80%94a%20set%20of%20physical,of%20transnational%20repression%20in%202024

[69] Lily Sparks & Kate Weine, "We Will Find You: A Global Look at How Governments Repress Nationals Abroad," *Human Rights Watch*, Feb 22 2024, accessed Mar 28 2025, https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad#:~:text=Human%20Rights%20Watch%20verified%20three,punishing%20or%20interrogating%20their%20family

[70] Ibid.

[71] Ibid.

For instance, in 2023, officials abruptly halted the publication of youth unemployment statistics after the jobless rate hit record highs, claiming a need to refine the methodology.[72] This move came amid a slew of weak economic indicators and was widely perceived as an attempt to conceal negative news. Authorities have also limited access to other economic data, from corporate registrations to academic journals, and cracked down on due diligence firms, thereby depriving the public and markets of transparency. By tightly managing economic narratives, the CCP aims to prevent financial anxieties from sparking broader public discontent.

Beijing's heightened sensitivities extend beyond economic data to encompass any information it considers politically "sensitive." This is evidenced by the case of Fu Cha (富察), a Taiwan-based publisher and commentator originally from mainland China. Fu Cha, whose real name is Li Yanhe, was detained by Chinese security agents during a trip to Shanghai in 2023 and later secretly tried for alleged national security offenses.[73] His apparent "crime" was sharing uncensored historical and political content with broader audiences outside mainland China. As the editor-in-chief of Gusa Publishing in Taiwan, Fu Cha published books on topics such as the Communist Party's history and the oppression of Uyghurs in Xinjiang – material that is heavily censored in China.[74] On 27 March 2025, a Shanghai court sentenced him to three years in prison on charges of "inciting secession, " underscoring the regime's zero tolerance for those disseminating information deemed hostile to its narrative.[75] Fu Cha's detention sends a

---

[72] Laurie Chen & Albee Zhang, "China suspends youth jobless data after record high readings," *Reuters*, Aug 15 2023, accessed Mar 28 2025, https://www.reuters.com/world/china/china-stop-releasing-youth-jobless-rate-data-aug-says-stats-bureau-2023-08-15/#:~:text=Aug%2015%20%28Reuters%29%20,largest%20economy

[73] "China: Authorities charge, detain journalists," *Federación Internacional de Periodistas*, May 4 2023, accessed Mar 28 2025, https://www.ifj.org/es/sala-de-prensa/noticias/detalle/article/china-authorities-charge-detain-journalists#:~:text=In%20a%20separate%20incident%2C%20after,in%20activities%20endangering%20national%20security%E2%80%9D

[74] Brian Hioe, "Fucha Sentencing Shows Efforts By China To Intimidate Taiwan," *News Bloom*, Mar 19 2025, Mar 28 2025, https://newbloommag.net/2025/03/19/fucha-sentencing/

[75] "China: Release Taiwan-based book publisher Li Yanhe," *Article 19*, Mar 28 2025, accessed Mar 28 2025, https://www.article19.org/resources/release-taiwan-based-book-publisher-li-yanhe/#:~:text=On%20Wednesday%2027%20March%2C%20a,with%20his%20family%20in%20Taiwan

clear warning to Chinese citizens and the diaspora alike that even interacting with overseas media or publishing critical content abroad can lead to severe punishment. This increased repression at home, fuelled by the regime's insecurity regarding economic and social stability, is choking the remaining avenues for truthful reporting and open discussion within China. Under mounting domestic strain, the state is intensifying efforts to silence any voices that might amplify inconvenient truths or alternative viewpoints.

6.3 Technological Reinforcement of Control through AI and "Smart Governance"

The Chinese government is harnessing cutting-edge technology – particularly artificial intelligence (AI) and big data analytics – to enhance its surveillance and censorship apparatus. In line with President Xi's vision of "smart governance", authorities are integrating massive data streams from cameras, online platforms, and other sensors into unified systems to better monitor the populace in real time.[76] One prominent development is the deployment of AI-driven surveillance software often referred to as "one person, one file." This technology automatically consolidates all data on an individual – from facial recognition camera footage to online activities – into a single, ever-updating dossier.[77] Such systems can identify and track people even if they wear masks or attempt to obscure their appearance, thanks to machine-learning algorithms that improve accuracy as data volume grows.[78] Security agencies can thus instantly access an individual's profile and even locate them geographically by cross-referencing live camera feeds with personal data, vastly increasing the state's capacity

---

[76] Ausma Bernot & Susan Trevaskes, "Smart Governance, Smarter Surveillance," *The China Story*, May 10 2022, accessed Mar 28 2025, https://www.thechinastory.org/yearbooks/yearbook-2021-contradiction/chapter-1-smart-governance-smarter-surveillance/#:~:text=People%E2%80%99s%20Republic%20of%20China%20,and%20economic%20development%2C%20ideology%2C%20and

[77] Eduardo Baptista, "Insight: China uses AI software to improve its surveillance capabilities," *Reuters*, Apr 8 2022, accessed Mar 28 2025, https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08/#:~:text=BEIJING%2C%20April%208%20%28Reuters%29%20,review%20of%20government%20documents%20shows

[78] Ibid.

to find "troublesome" citizens or dissidents. As one analysis notes, these AI tools constitute a pervasive surveillance dragnet that could enable authorities to pre-empt protests or dissent "before they start" by detecting patterns and anomalies in citizens' behaviour.[79]

Beyond domestic surveillance, China's techno-authoritarian toolkit is also directed outward. Sophisticated AI-powered censorship algorithms now trawl global Chinese social media and communication platforms, ensuring that politically sensitive content (from mentions of Tiananmen to satire about leaders) is swiftly deleted or suppressed. Tech companies like Tencent, which operates WeChat, cooperate closely by censoring users and sharing data with the government, even for accounts registered overseas.[80] Recent advancements, such as China's DeepSeek AI model, further bolster its ability to analyse vast troves of text, images, and biometric data for any sign of dissent or subversion, according to research by the National Endowment for Democracy.[81]

6.4 Breakdown of Conventional Mitigations: Hong Kong and Business Autonomy

Beijing's recent actions have also undermined mechanisms that once provided limited insulation for information freedom and external engagement. The "One Country, Two Systems" framework in Hong Kong – long promoted as a means to maintain a freer environment and attract Western collaboration – has effectively collapsed as the Chinese state prioritised political control over openness. The clearest example is China's imposition of the Hong Kong National Security Law (HKNSL) in Hong Kong in 2020, bypassing local legislative process and scrutiny. The HKNSL introduced severe penalties for broadly defined offenses like subversion and collusion with foreign forces

---

[79] Lin Yueyang, "China's homegrown tech boosts global surveillance, social controls: report," *Radio Free Asia*, Feb 20 2025, accessed Mar 28 2025, https://www.rfa.org/english/china/2025/02/20/china-ai-neuro-quantum-surveillance-security-threat/#:~:text=China%E2%80%99s%20increasingly%20powerful%20AI%20surveillance,wrote%20report%20author%20Valentin%20Weber

[80] Sparks & Weine, "We Will Find You."

[81] Lin, "China's homegrown tech boosts global surveillance."

and has been used to arrest journalists, shut down independent media, and silence protesters.[82] Western governments and human rights experts at the United Nations view these measures as a blatant violation of the promised autonomy and freedoms in Hong Kong following international human rights treaties.[83] Indeed, any remaining trust in "One Country, Two Systems" as a viable model has evaporated amid Beijing's overreach. The push to finally implement a local Article 23 security law, formally titled as "Safeguarding National Security Ordinance" (SNSO) – with even more provisions to curb dissent – is seen as a transplantation of China's national security regime, norms and practices into Hong Kong.[84]

Far from reassuring foreign partners, this overreach has alienated them: the United States, for example, declared the erosion of Hong Kong's autonomy a threat to international business confidence and responded by sanctioning officials and warning companies of risks to operating under the new regime.[85] In short, what was once a semi-open conduit between China and the world is now tightly controlled, closing off an avenue that had mitigated China's information isolation.

The Hong Kong episode underscores how the Chinese state's drive to control information and society now extends to the region that international business once regarded as distinctive from China.[86] This heavy-handed tactic undermines the assurances that Hong Kong's distinct system, especially the common law system

---

[82] "Tracking the Impact of Hong Kong's National Security Law," *China File*, Nov 14 2024, accessed Mar 28 2025, https://www.chinafile.com/tracking-impact-of-hong-kongs-national-security-law

[83] Yan-ho Lai, "Not Just About the Law: Reflections on A Report on the National Security Regime in Hong Kong (2024)," *Taiwan Human Rights Journal* (7), no. 4 (2024): 89-109.

[84] Eric Y.H. Lai, "Implications of Article 23 Legislatgion on the Future of Hong Kong," *The Jamestown Foundation*, Mar 1 2024, accessed Mar 28 2025, https://jamestown.org/program/implications-of-article-23-legislation-on-the-future-of-hong-kong/

[85] Cari Stinebower, Steven Grime & David Houck, "U.S. Expands Sanctions Against Hong Kong Officials, Including Chief Executive Carrie Lam; White House Issues Executive Orders Targeting WeChat and TikTok," *Winstron & Strawn*, Aug 7 2020, accessed Mar 28 2025, https://www.winston.com/en/blogs-and-podcasts/global-trade-and-foreign-policy-insights/us-expands-sanctions-against-hong-kong-officials-including-chief-executive-carrie-lam-white-house-issues-executive-orders-targeting-wechat-and-tiktok

[86] For further details of the state of information freedom in Hong Kong, read Resilience Innovation Lab's latest report "Safeguarding Freedom of Information in Hong Kong: Challenges, Opportunities and Remedies", March 2025.

inherited from the British colonial rule, was meant to provide to global investors. It also illustrates that in China's current environment, *any* activity – whether in media, academia, or commerce – can be considered a security threat if it strays from Party objectives. The breakdown of these traditional safeguards (Hong Kong's semi-autonomy and the relative independence of Chinese-linked businesses) results in fewer safety valves or moderating influences to slow the decline of information freedom. Where the appeal of Hong Kong's freedoms once facilitated China's engagement with the liberal world, and private business actors could occasionally serve as bridges, those channels are now closing under pressure from the Chinese communist regime.

7. Conclusion and Recommendations

Overall, the outlook for information freedom in China appears to be depressing. China's digital landscape is experiencing ever-intensifying state control over information and communication. The intersection of rising geopolitical tensions, heightened insecurity within the Chinese regime, and rapid advancements in surveillance technologies suggests that this restrictive trend is poised to deepen further in the coming years. As governmental capabilities to monitor and constrain digital spaces grow, opportunities to access uncensored information will continue to shrink, posing significant challenges for global stakeholders in an increasingly interconnected world.

Under the combined weight of geopolitical tensions, domestic insecurity, high-tech surveillance, and the CCP's aggressive interference in formerly autonomous spheres, the space for free expression and independent information in China is rapidly contracting. All signs indicate that the ruling authorities will continue this trajectory, prioritising regime security over openness. This grim reality demands greater attention from international stakeholders – governments, businesses, and civil society – who have interests in China's society and markets. Without concerted scrutiny and pushback, Beijing's tightening grip on information will only strengthen, profoundly impacting not just the rights of the Chinese people, but also global knowledge flows and the principles of a free and open exchange of ideas. The business environment in China has become increasingly closed and unfair, as Chinese authorities and domestic companies enjoy significantly greater access to information on the mainland than their foreign counterparts. This situation is particularly ironic given that China remains an active member of the World Trade Organisation, yet unfair competition persists in the Chinese market due to the unequal access to information between China and the West. Those concerned must recognise the severity of these challenges and consider how to resist or at least slow the march toward an increasingly closed and controlled information environment in China.

While near-term prospects for greater openness in China's digital environment appear limited, there remains an urgent need for coordinated action among international governments, institutions, businesses, and civil society organisations. Such collaboration is essential to mitigate risks and uphold international standards of information freedom.

7.1 State Actors

National governments should embed digital rights and information freedom into their legislative frameworks to effectively respond to China's tightening grip on digital spaces. A crucial initial measure would be incorporating explicit human rights clauses within trade agreements and diplomatic interactions, accompanied by annual assessments of China's digital policies. Although these assessments alone may not constitute comprehensive due diligence, they offer essential accountability mechanisms and diplomatic leverage to advocate greater transparency and adherence to international standards.

7.2 Multilateral Institutions

Multilateral organisations, including the World Bank (WB), the International Monetary Fund (IMF), and the World Trade Organization (WTO), should develop guidelines promoting regulatory standards that emphasise open access to information. It is essential to strengthen international mechanisms tasked with monitoring and reporting digital repression in China to maintain consistent global attention and coordinated action on this issue.

7.3 International Business Sector and Multinational Corporations (MNCs)

Companies operating in China face escalating risks due to intensifying digital restrictions, with foreign firms particularly experiencing increased hostility. To safeguard their operations and personnel, multinational corporations (MNCs) should conduct ongoing risk assessments to closely monitor evolving conditions within China's digital environment. Given the widespread uncertainty businesses face when managing these risks, Chambers of Commerce and industry associations should collaborate in creating

platforms for information exchange and practical risk assessment toolkits. Such initiatives will equip companies with informed strategies for navigating China's progressively restrictive digital landscape.

Moreover, businesses should commit to responsible investment principles as outlined in a Business and Human Rights (BHR) Charter. This commitment would ensure companies align their operations with internationally recognised human rights standards and proactively mitigate risks associated with digital repression. By emphasising transparency and collaboration, the private sector can significantly contribute to resisting China's digital authoritarianism, thereby protecting both human rights and commercial interests.

7.4 Global Civil Society and Academic Institutions

Civil society organisations (CSOs), media outlets, and academic institutions should assume a more proactive role in preserving and disseminating critical information at risk of censorship in China. Media organisations and investigative journalists need to actively support Chinese community organisers, trade unionists, activists, and independent journalists, providing them with essential resources and networks to help navigate state-imposed restrictions effectively.

Academic institutions carry a distinct responsibility to safeguard historical and contemporary records vulnerable to censorship or erasure. By systematically archiving essential data and conducting rigorous research into China's digital environment, universities and research institutes can ensure vital information remains available for future generations. Additionally, collaborative partnerships between international scholars and Chinese researchers in exile can foster valuable knowledge exchange and facilitate the development of strategies aimed at countering digital censorship.

This is the end of the report.