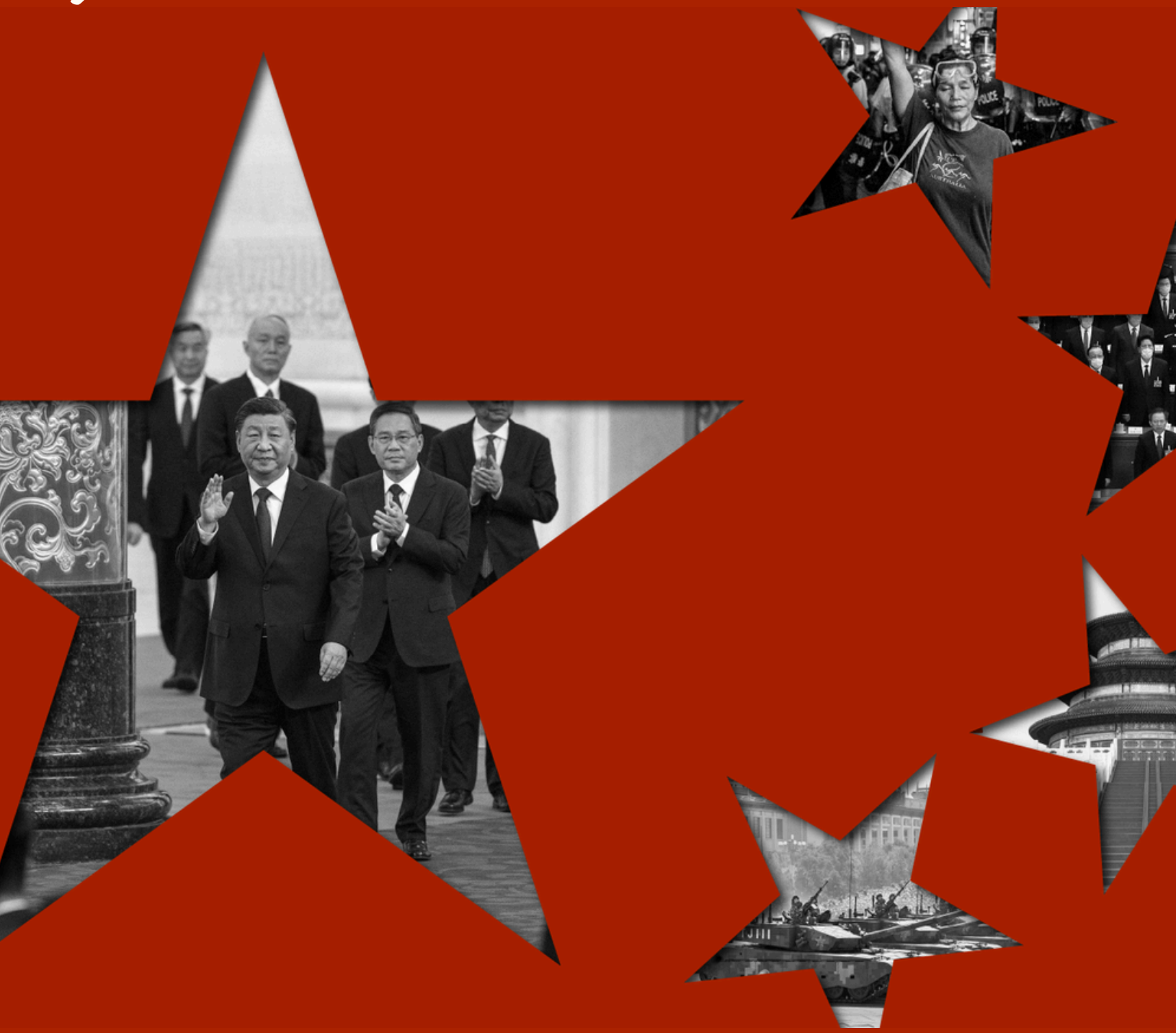
Jamestown

March 6, 2026



China Brief

Volume 26, Issue 5

In This Issue

China Brief

Notes

APEC Leaders in 2014, when Xi Jinping last hosted the organization's annual summit.
(Source: Wikipedia)

Beijing Revives Asian Values in Regional Push

Arran Hope
March 6, 2026

Executive Summary

- The People's Republic of China (PRC) is focused on deepening influence in its neighborhood. As this year's APEC host, it sees an opportunity to drive its regional agenda through multilateral institutions.
- General Secretary Xi Jinping, informed by Party theorists, is promoting "Asian values" to advance PRC discourse power. This understanding of "Asian values" is explicitly anti-Western, pro-authoritarian, and sees the Party's interests as synonymous with those of the entire region.
- Leader's speeches, authoritative policy documents, and other official publications constantly link success in achieving the Party's regional ambitions with expanding Beijing's power globally.

This year, the People's Republic of China (PRC) is the host country for the Asia-Pacific Economic Cooperation (APEC) organization. Beijing views the inter-governmental forum, which consists of 21 member economies—including four in the Americas—as a key multilateral institution for regional development. It also sees itself as the central node that drives that development: Chinese leader Xi Jinping has analogized the PRC's relationship with the region to a sweet potato plant, in which the nutrient-rich tubers at the base fuel "vines that extend in all directions" (藤蔓向四面八方延伸) (People's Daily, October 25, 2025). At the same time, the Party views the forum as an important platform for advancing its strategic goals in its own neighborhood, which, according to Chinese Communist Party (CCP) theorists and senior officials, is a launchpad for its global ambitions.

First Asia, Then the World

In a speech to APEC leaders last November, CCP General Secretary Xi Jinping praised the Asia-Pacific region, recognizing it as the "most dynamic" (最具活力) part of the world economy" (Xinhua, November 1, 2025). In the run up to his speech, the People's Daily said the quiet part out loud. Promoting the PRC's centrality to the region, it proclaimed that "in the grand symphony of the 'Asia-Pacific miracle,' the 'Chinese miracle' is its most inspiring chapter" (在"亚太奇迹"的宏大乐章中，"中国奇迹"是其中最激昂的篇章). It also claimed that "the world sighs gratefully, 'the planet needs a leader like Chairman Xi'" (世界感叹，"全球需要像习主席这样的领导人"). For the Party, attacking the West is key to advancing its own interests in the region.

The article was full of such rhetoric: Noting that the region accounts for a third of global population, over 60 percent of the world's economic output, and nearly half of its trade volume, it framed it as an "important battleground" (重要阵地). It also framed the PRC system as a better model for global governance, calling for the Party to continue using Chinese-style modernization "to promote and implement the modernization of countries throughout the world" (推动实现世界各国的现代化) (People's Daily, October 25, 2025).

Promoting economic development is core to the Party's stated agenda for the region. Vice Minister of Foreign Affairs Ma Zhaoxu (马朝旭), an accomplished and seasoned diplomat who is set to run the table at many of the APEC events this year, has made this clear. His stated focus for APEC in 2026 is to "build an Asia-Pacific community of common destiny and promote common prosperity" (建设亚太共同体，促进共同繁荣) through a focus on opening up, innovation-driven development, and cooperation (MFA, December 12, 2025, accessed February 18). But Ma, too, has broader ambitions. In a February speech, he argued that the PRC's hosting of APEC this year "has significance … far beyond the Asia-Pacific region" （意义 … 远远超出亚太范畴) (People's Daily, February 9).

Linking regional success through APEC to increased global influence for the CCP is common in Party-state discourse. For instance, a December 2025 article for the magazine Modern World (当代世界), a publication supervised by the Party's International Liaison Department, argued that the PRC should use hosting APEC to "enhance [the PRC's] discourse power and create a new pattern for the international economy and trade" (提升话语权、打造国际经贸新格局) (Modern World, December 2025). **[1]**

Good Neighborliness as Strategic Priority

As dialectical materialists, Party leaders see economic influence as fundamental to its regional clout. The Party nevertheless is also pursuing alternative methods to shift the balance of power in the Asia-Pacific. To do so, it is focusing on its "neighborhood" (周边), or periphery. As the scholar Dylan M.H. Loh has observed, Southeast Asia "is, and continues to be, the space where Chinese diplomacy is most visible and active as part of Beijing's renewed focus on its periphery diplomacy" (Loh, 2025). **[2]**

The PRC has hosted APEC on two previous occasions, once in 2001 and again in 2014, leading to the adoption of the Shanghai Consensus (上海共识) and the Beijing Platform (北京纲领), respectively. In late 2013, just before assuming the role of APEC host, Xi Jinping chaired a conference on "neighborhood diplomacy work" (周边外交工作). He emphasized that the region held "extremely important strategic significance" (具有极为重要的战略意义) for the PRC (Xinhua, October 25, 2013). A similar pattern held this time around, with the Party holding a "Central Conference on Work Related to Neighboring Countries" (中央周边工作会议) in 2025. This time, Xi's remarks focused much more on his personal foreign policy agenda: the need to build a community of common destiny (CCD) with neighboring countries, promote the One Belt One Road initiative, and advance an "Asian security model" (亚洲安全模式) (MFA, April 9, 2025).

Emphasis on the country's neighborhood is apparent in the Party-state's highest-level policy documents. The draft of the 15th Five-Year Plan, released in early March, frames the PRC's neighbors as key assets in its bid to build a "new type of international relations" (构建新型国际关系). Assessing that "great power rivalry has become more complex and intense" (大国博弈更加复杂激烈), the Party seeks to "gain the strategic initiative in fierce international competition" (在激烈国际竞争中赢得战略主动). Its strategy for doing so rests in part of "deepening development integration with neighboring countries … and building a [CCD] for [its] neighbors" (深化周边发展融合，强化共同安全，巩固战略互信，构建周边命运共同体) (Xinhua, March 5).

Courting Neighbors With 'Asian' Values

Central to Beijing's approach to neighborhood diplomacy are "Asian values" (亚洲价值观), which Xi stated should be taken as the region's fundamental principles (MFA, April 9, 2025). Discussion of "Asian values" was a staple of international relations discourse in the 1990s. The debate was often crude, reducing the world into antagonistic normative domains, and has been largely dismissed in the 21st century. As the scholar Amartya Sen remarked at the time, "the so-called Asian values that are invoked to justify authoritarianism are not especially Asian in any significant sense. Nor is it easy to see how they could be made into an Asian cause against the West, by the mere force of rhetoric" (Sen, 1997). **[3]**

The CCP is nevertheless seeking to revive the idea, and is promoting its own values as a stand-in for those of the continent. The intellectual home for this drive appears to be the China Institute of International Studies (CIIS), a think tank under the Ministry of Foreign Affairs, which has devoted considerable attention to the topic in recent years. Writing in the Global Times in 2023, CIIS researcher Xiang Haoyu (项昊宇) argued that Asian values were being given "new contemporary meaning" (新的时代内涵). In Xiang's reading, however, Asian values appear to be synonymous with CCP governance practice. For instance, he argues that they advocate "maintaining social stability and order through strong political systems and promoting rapid

economic and social development through strong government leadership" (通过强有力的政治体制来维持社会的稳定和秩序，通过政府的强力领导推动经济社会快速发展来达到改善民生的目标). He even suggests that Xi's Global Civilization Initiative "is in fact an interpretation and sublimation of 'Asian values' under new circumstances (正是对新形势下"亚洲价值观"的阐释和升华). He also makes clear that "Asian countries need to break free from the ideological confrontation trap set by the West" (亚洲国家需要跳出西方设定的意识形态对抗的话语陷阱), arguing that Asian values "still have instinctive appeal for most Asian countries in the face of Western ideological infiltration" (依然是多数亚洲国家面对西方意识形态渗透时的本能诉求) (Global Times, July 6, 2023).

Other CIIS scholars have put forward similar arguments. The deputy director of CIIS's Institute of Asia-Pacific Studies has written that "Asian" values have "entered a period of reconstruction" (进入重构期) as the PRC has risen to the center of the world stage. Demonstrating how Beijing links success in its neighborhood to achieving its ambitions globally, Du goes on to predict that "Asian" values will contribute "a new paradigm" (新范式) to global governance (Xi Jinping's Diplomatic Thought and China's New Era Diplomacy, June 16, 2025). A third CIIS scholar heralds a degree of success in Beijing's promotion of Asian values. Liu Qing (刘卿) notes that the PRC is formalizing "Asian" values in official documents, such as joint statements with Malaysia, Laos, Indonesia, and Cambodia (People's Tribune, November 3, 2025). Linking Asian values to Confucianism, the "China model," and Beijing's merging of security of development, Liu also argues that "Asian" values have become "an important symbolic concept" (重要标识概念) in Xi's neighborhood diplomacy (China Brief, May 23, 2025).

Liu Qing also discusses Asian values in the context of building various CCDs. To date, he claims, the PRC has formed two major clusters of CCDs, in the Indochina Peninsular and Central Asia, in addition to various bilateral CCDs. Other scholars make this link too. In an article funded by the Chinese Academy of Social Sciences, the international relations scholar Zheng Xianwu (郑先武) writes that Beijing is constructing a "multi-layered community of common destiny" (多层次命运共同体) in which the Asian CCD is an important component of surrounding CCDs as part of a cooperation framework that connects sub-regional, trans-regional, and bilateral/multilateral entities (Modern World, January 26). **[4]**

Conclusion

Beijing appears to believe that it is having some success in building its influence in Southeast Asia. Hosting APEC this year will provide it with additional opportunities to steer narratives and guide cooperation in its favor. it is less clear, however, that the rest of the region is receptive to its values-based pitches and hardline rejection of the West. In April 2025, the ISEAS – Yusof Ishak Institute in Singapore published an annual survey, "The State of Southeast Asia." Among more than 2,000 respondents in the region canvassed in the first six weeks of the year, the PRC's aggressive behavior in the South China Sea was ranked as the region's top geopolitical concern; and in its analysis of the responses, the survey report's authors wrote that despite the PRC's positive standing, "the region's concern about [the PRC's] growing economic and political-strategic influence outweighs its acceptance." It also noted that the United States had "overtaken China to become the prevailing choice if the region were forced to align itself with one of the two strategic rivals" (Seah, S. et al., April 3, 2025). **[5]** These responses may change in this year's survey, which is yet to be published. But it provides one indication that Beijing still faces an uphill battle in its pursuit of regional dominance.

Observers in the West can dispute, or even deride, some of Beijing's attempts to draw the region closer into its orbit. But the logic behind Beijing's primary focus on the region is sound. Constituting a significant portion of the world's population, economic dynamism, and trade volume, Southeast Asia will likely be central to global prosperity in the decades to come. Absent persistent engagement with the region, however, Xi Jinping's "sweet potato plant" will find fertile soil in which to grow, and its multi-layered CCDs space to expand.

Arran Hope is the editor of China Brief at The Jamestown Foundation.

Notes

[1] The research for this article in Modern World was supported by a grant funded by the PRC Ministry of Education.

[2] Dylan M.H. Loh, China's Rising Foreign Ministry, Stanford University Press, 2025

[3] Amartya Sen, *Human Rights and Asian Values*, Carnegie Council on Ethics and International Affairs, 1997.

[4] Like other scholars, Zheng appears to see Chinese and Asian interests as synonymous, noting that "Asian" values "had distinct Chinese characteristics from their inception" (初创之时便具有鲜明的中国特质).

[5] Seah, S. et al., The State of Southeast Asia: 2025 Survey Report (Singapore: ISEAS - Yusof Ishak Institute, 2025).

To read this article on the Jamestown website, click here.

Chinese delegates listen to a speech during the opening session of the National People's Congress. (Source: Kevin Frayer/Getty Images)

New PRC Cybercrime Law Heralds Digital Iron Curtain

Youlun Nie
March 6, 2026

Executive Summary

- The Ministry of Public Security's draft Cybercrime Prevention and Control Law marks a seminal shift from reactive policing to preventive governance, codifying a regulatory system designed to eliminate all remaining digital gray zones.
- By outlawing privacy-enhancing tools based on function rather than intent, enforcing real-name registration down to the network infrastructure layer, and nationalizing the discovery of cybersecurity vulnerabilities, the legislation effectively eradicates technical anonymity and centralizes state control over critical zero-day resources.

Executive Summary (continued)

- The draft leverages administrative power through exorbitant fines and extrajudicial detention, enabling public security bureaus (PSBs) to bypass the formal justice system and impose crippling penalties on ordinary netizens, technical facilitators, and private enterprises.
- Projecting control globally, the legislation formalizes border controls and authorizes the freezing of assets linked to "fake information," providing a robust domestic legal foundation for transnational repression against foreign entities, international personnel, and the Chinese diaspora.

Digital governance in the People's Republic of China (PRC) is poised to enter a new phase. On January 31, the Ministry of Public Security (MPS) released the Cybercrime Prevention and Control Law (Draft) (网络犯罪防治法 (征求意见稿)) for public comment (MPS, January 31). **[1]** Recognizing that technical blockades are no longer sufficient, Beijing is building a robust legal framework to expand and codify its digital control apparatus. For over two decades, the Great Firewall (GFW)—an umbrella term for the PRC's Internet censorship systems—has served as the primary instrument of digital control. **[2]** The draft law shifts the regulatory focus from technical censorship operations to substantive legal sanctions.

According to the "explanation" (说明) that accompanied the MPS's draft law, the rapid development of the Internet has facilitated the migration of traditional crimes online, forming "massive and deeply entrenched black and grey industrial chains" (体系庞大、盘根错节的黑灰产业链条) (MPS, January 31). The authorities concede that reactive enforcement for individual cases cannot halt increasing cybercrime. In response, the proposed legislation establishes an operational doctrine crackdowns with prevention, prioritizing prevention, governing the ecology, and collaborative linkage" (坚持"打防结合、防范为先、生态治理、协同联动"的原则).

This official emphasis on "prevention" and "ecological governance" reflects a broader Party-state logic of "source governance" (源头治理). A key feature of the Party's approach to social management (it received mentions in both the 12th Five-Year Plan and the 18th Party Congress report), source governance focuses on preemptively dealing with social problems before they emerge or escalate (National Development and Reform Commission, September 2011; Xinhua, November 8, 2012; Party Members' Net, February 25, 2013). **[3]** Although the draft is ostensibly aimed at combating telecom fraud and online gambling, it uses these issues as a pretext to neutralize perceived threats, including unauthorized technological capabilities and the networks of citizens who rely on them.

By defining the "evasion of supervision systems" (规避监管) as a punishable offense, the draft targets a broad ecosystem of technical facilitators and independent researchers, not just the users of privacy-enhancing tools. Beyond domestic surveillance, it also empowers police authorities to impose exorbitant administrative fines and administrative detention, which bypasses judicial oversight, while formalizing long-arm jurisdiction to threaten foreign entities, individuals, and the Chinese diaspora.

Elimination of Gray Zones

To eliminate the remaining digital gray zones that threaten Party-state interests, the draft law systematically targets the entire ecosystem of digital circumvention. It establishes strict legal prohibitions on privacy-enhancing tools and their technical facilitators, eradicates network-

level anonymity, and centralizes state control over cybersecurity vulnerabilities.

The official rationale frames the draft law's sweeping prohibition of privacy and circumvention tools as necessary to cut off the "material supply and technical support" (物料供应、技术支持) components of the cybercrime ecosystem. By formalizing a blanket ban on such technologies, it marks a definitive shift from targeting illicit online behavior to penalizing the underlying tools themselves. In doing so, it ends any lingering pretense of technical neutrality. Article 14 explicitly forbids any individual or organization from engaging in the "illegal production, sale, provision, or use" (非法制作、销售、提供、使用) of restricted tools. Specifically, Item 6 of the article introduces a sweeping prohibition against equipment, software, or services "specifically used to commit cyber illegalities and crimes or having the function of evading supervision systems" (专门用于实施网络违法犯罪或者具有规避监管制度功能的设备、软件、工具、服务). In the PRC's legal lexicon, "supervision" encompasses the totality of the state's monitoring apparatus, including real-name registration and GFW filtering. Therefore, privacy-enhancing technologies (PETs), such as virtual private networks (VPNs) and end-to-end encrypted messaging applications, have become strictly prohibited. By relying on a function-based standard, the legislation lowers evidentiary thresholds for police action, removing the need to prove criminal intent. Of particular concern, this functional ban poses an operational threat to international businesses that rely on corporate VPNs for secure cross-border communications. Because the draft offers no explicit exemptions for legitimate commercial use, multinational companies face a stark dilemma: either risk massive legal liability or transition to state-approved, monitored network channels that compromise their proprietary data.

Beyond targeting end-users, the regulatory dragnet extends to the very ecosystem that supports Internet freedom, explicitly penalizing technical assistance for accessing "illegal information" (违法信息) from abroad. Article 44 codifies the GFW's operations into formal law, mandating that network operators block illicit information originating from outside the PRC. Crucially, it prohibits individuals and organizations from supplying technical tools or services that help others circumvent information controls to access or share blocked content. The stipulation is designed to disrupt the networks of developers, tutorial writers, and technical enthusiasts who have historically connected the Chinese intranet to the global Internet. By outlawing the act of "helping" others access blocked content, the state aims to isolate Chinese people within a strictly monitored national network. This turns a common technical workaround into a high-stakes legal risk.

To enforce these prohibitions, the draft law integrates real-name registration from the application layer down to the physical and network infrastructure, eliminating digital anonymity in the process. Articles 11–13 prohibit the disruption of real-name management systems. Specifically, Article 12(3) outlaws IP address switching tools, batch phone card control tools, and other means to evade network operators' account registration review rules. The clause precisely targets dynamic IP proxies or jumping servers. This creates a one-to-one mapping between a user's physical identity and their digital footprint, making technical anonymity virtually impossible to achieve. For activists and dissidents who rely on IP obfuscation to avoid detection, the measures represent a closing of the final technical loopholes used for safe communication.

Parallel to restricting circumvention tools, the state is moving to monopolize the discovery of

network vulnerabilities to ensure the security apparatus maintains an offensive edge in cyberspace. Articles 24–25 impose a strict administrative approval regime on "white hat" security research and penetration testing: Independent researchers are now prohibited from conducting "network security vulnerability probing and penetration testing" (网络安全漏洞探测、渗透性测试) on critical systems (level three and above), without explicit approval from provincial-level cyberspace administrations or public security bureaus (PSBs), or authorization from industry regulators or network operators. **[4]** Furthermore, the draft mandates that even authorized testing must be "reported to county-level and higher public security organs five working days prior to the implementation of the activity" (在活动实施五个工作日前向县级以上公安机关报告). Coupled with Article 24's ban on the unauthorized "discovery, collection, and publication of network product vulnerabilities" (网络产品安全漏洞发现、收集、发布等), the strict prior notification mechanism would ensure that the Party-state has first access to newly discovered flaws. Such hoarding of technical vulnerabilities not only stifles independent cybersecurity innovation but also increases the systemic risk to global supply chains, as these flaws may be weaponized as zero-day vulnerabilities for state-sponsored espionage or domestic surveillance before they can be patched.

Weaponization of Administrative Penalties

In the PRC legal system, administrative violations encompass a wide spectrum of offenses, including acts that would be classified as misdemeanors, or even felonies, in Western jurisdictions. **[5]** A critical difference, however, is that PSBs are the main adjudicators of these penalties. The draft law categorizes digital circumvention as a severe administrative offense, empowering the police to impose exorbitant fines and arbitrary detention. Because these measures inherently lack judicial review, their expanded use effectively bypasses the formal justice system. This creates a parallel mechanism that cripples targeted individuals and generates lucrative revenue streams for local governments.

This administrative expansion aligns directly with the MPS's goal, stated in its explanation, to "move regulatory checkpoints forward to strengthen administrative supervision" (做到关口前移，强化行政监管). By shifting enforcement to the administrative level, the draft law establishes a system of "fiscal policing," whereby punitive financial penalties can target anyone attempting to bypass censorship without formal criminal trials. The draft introduces a structure of cascading fines that punishes activities even when they generate "no illegal income" (没有违法所得). Under Article 57, anyone who evades real-name registration, including through using foreign SIM cards or IP proxies, faces fines of up to RMB 200,000 ($29,000). Authorities can also place violators on a blacklist, restricting their access to basic telecommunications and financial services. Moving up the chain, Articles 58 and 59 empower police to impose fines of up to RMB 500,000 ($72,500) on non-profit activists, open-source developers, and digital rights defenders who produce or provide circumvention tools. This represents a massive escalation from previous regulations, providing the state with a low-cost mechanism to paralyze dissenters and enforce compliance while avoiding the international scrutiny often triggered by criminal prosecutions.

Beyond inflicting financial ruin, the draft law institutionalizes extrajudicial detention for the immediate physical removal of targets. Articles 57–61 uniformly empower PSBs to impose up to 15 days of "administrative detention" (拘留) for violations under "serious circumstances" (情节严重的)—a threshold left strategically vague. Such

discretionary power enables the rapid removal of perceived troublemakers from society during sensitive political periods. Administrative detention in the PRC requires no prosecutorial approval and no court appearance, thus enabling the system to focus on "preventive" suppression. Consequently, the state drastically lowers the evidentiary threshold required to strip citizens of their liberty.

Complementing these individual sanctions, the law expands the corporate liability regime that forces telecommunications, financial, and Internet service providers to serve as the front-line enforcers of state regulations. Article 60 mandates that service providers who "fail to fulfill cybercrime prevention and control obligations" (未落实网络犯罪防治义务), including the failure to monitor, discover, and block illegal information, can face enterprise fines of up to RMB 5 million ($725,000). Simultaneously, the "directly responsible personnel" (直接负责的主管人员) face personal fines of up to RMB 200,000 ($29,000). The mandate ensures that companies across these critical sectors must internalize the state's surveillance mission to guarantee their own survival. Fear of these massive penalties will inevitably lead to over-compliance, where firms implement censorship and monitoring regimes even more robust than those explicitly required by law.

The result is a governance model where the distinction between criminal and administrative law is blurred to the advantage of the security services. Police authorities can now ignore procedural safeguards in the criminal code by employing administrative penalties instead. Crucially, the framework creates incentives that enforcement units, particularly those under fiscal strain, may exploit for revenue generation. The ability to levy massive fines on digital infractions allows local governments to target ordinary citizens and private enterprises to supplement depleted budgets (China Brief, February 3).

Lawfare and Long-Arm Jurisdiction

To project its digital censorship and deterrence capabilities globally, the draft law establishes a comprehensive framework for lawfare and long-arm jurisdiction. This extraterritorial expansion provides domestic legal cover for transnational repression, asset weaponization, and the policing of global discourse.

The draft's explanation explicitly notes the transnational nature of modern cybercrime, mandating measures for "cross-border cybercrime sanctions and the supervision of cross-border network services" (跨境网络犯罪制裁、跨境网络服务监管). Under Article 54, authorities can "seal, seize, and freeze" (查封、扣押、冻结) and ultimately "confiscate" (没收) the criminal proceeds—as well as any enterprises, securities, or real estate invested with those proceeds—of foreign entities and individuals deemed to have committed cybercrimes, and can further restrict their direct or indirect investments. The provision poses a substantial operational risk to multinational corporations and investors. If a foreign entity is accused of violating the new cyber regulations, its legitimate business revenues and investments could easily be reclassified as "criminal proceeds," leading to the immediate expropriation of its assets. The threat of expropriation transforms foreign investment in the PRC into a mechanism that ensures compliance with Beijing's digital dictates.

Alongside the confiscation of criminal proceeds, Article 55 directly targets "overseas institutions, organizations, and individuals" (境外机构、组织、个人) who manufacture or spread "fake information" (虚假信息) that damages the PRC's "national sovereignty, security, development interests, or public interests" (国家主权、安全、发展利益或者公共利益). Such broad wording

introduces long-arm jurisdiction that can easily be weaponized against political speech. The Party-state defines "fake information" as reporting or analysis that contradicts its official narrative, including reports on the human rights situation in Xinjiang, Xi Jinping's policy failures, or the PRC's structural economic challenges. This clause is a direct legal tool against overseas political dissidents, circumvention facilitators, non-governmental organizations, and media organizations. The provision authorizes the freezing of assets, entry bans, and the restriction of direct or indirect investments in the PRC. This not only infringes upon the property rights of overseas entities but also constitutes a textbook case of transnational repression against dissidents, subjecting ordinary individuals to the same sanctions previously used against U.S. Secretary of State Marco Rubio (PRC Ministry of Foreign Affairs, July 13, 2020, August 10, 2020).

In tandem with these measures, the draft law weaponizes border controls to punish both domestic and international targets. Article 56 grants "municipal-level and higher PSBs" (设区的市级以上公安机关) the power to impose an additional six-month to three-year "exit ban" on PRC citizens after they have completed criminal sentences for cyber-related offenses. The law simultaneously authorizes "relevant competent departments" (有关主管部门) to ban the entry of foreign personnel who violate the provisions of Chapter III of the draft law. This dual-track system creates tailored risks: for foreign executives, technical experts, and researchers traveling to the PRC, past digital activity could be used as a legal pretext to deny them entry as part of a broader strategy of political coercion; for the Chinese diaspora—including foreign permanent residents—returning to the PRC risks becoming a one-way trip, as their overseas digital footprint could trigger criminal penalties and subsequent exit bans.

Conclusion

The draft Cybercrime Prevention and Control Law is poised to drop a legal iron curtain over the PRC's digital landscape. It signals Beijing's intent to transcend mere technical filtering, codifying instead a system of absolute "preventive governance." By proposing to empower PSBs with unchecked administrative authority, the Party-state seeks to formally eradicate the last remaining digital gray zones. If enacted, this architecture would subordinate the judicial process to the brute force of administrative policing, ensuring that any attempt to bypass state surveillance is met with immediate extrajudicial suppression.

For the United States and the broader international community, the legislation's externalities demand immediate attention. The draft illustrates how Beijing intends to weaponize its domestic legal apparatus for global coercion. The proposed hoarding of network vulnerabilities would directly degrade global cybersecurity, while the expansion of long-arm jurisdiction would hold foreign capital, foreigners, and the Chinese diaspora hostage to the Party-state's political red lines. The public comment period closed on March 2, paving the way for the draft to be submitted to the National People's Congress (NPC). Given its inclusion in the legislative plan, formal enactment is likely by late 2027—prior to the conclusion of the current legislative term. While the ongoing legislative review and pushback—such as from economic agencies aiming to accommodate foreign investment—may soften certain implementation details, the overarching mandate of "preventive governance" will undoubtedly remain intact. As this framework advances toward implementation, foreign entities must recognize that the era of regulatory ambiguity is over. Engaging with the PRC's digital ecosystem will soon carry unprecedented legal, financial, and physical risks.

Youlun Nie is a commentator on Chinese affairs and a former Professor at East China Normal University, where he specialized in Chinese constitutional law and political institutions. He holds a Ph.D. in Law and has published extensively in academic journals on China's legal reforms. Currently, he focuses his research on the political rhetoric of the Chinese Communist Party and the instrumentalization of law in China.

Notes

[1] Observers have criticized the MPS's leading role in drafting this legislation, arguing that it inevitably expands police power by allowing the agency to act as both the architect and enforcer of the law. While this criticism is entirely valid, such a dynamic reflects standard legislative practice in the PRC. With the exception of major, cross-departmental laws, drafting responsibilities are routinely delegated to the functional ministry overseeing the specific portfolio. In the legislative plan of the 14th National People's Congress (NPC), the State Council was tasked with drafting the Cybercrime Prevention and Control Law, which it subsequently subcontracted to the MPS as the primary agency in charge. See Gazette of the Standing Committee of the National People's Congress (全国人民代表大会常务委员会公报), 2023, No. 6, p. 773.

[2] For detailed research into how the GFW operates, see the blogposts and papers published by Great Firewall Report, at https://gfw.report/en/.

[3] For more on the Party's approach to social management techniques, and how it links to its national defense mobilization system, see Samantha Hoffman, Mobilizing the State, (Washington, D.C.: The Jamestown Foundation) 2025 (forthcoming).

[4] The PRC has five levels of information security based on the potential consequences of damages to information systems (see KPMG China, May 2019; DataGuidance, February 10, 2023).

[5] Unlike Western legal systems, which generally process misdemeanors and felonies through the judicial branch, the PRC employs a bifurcated sanctioning system. Because the statutory thresholds for formal prosecution under the Criminal Law (刑法) are relatively high, a wide range of offenses—including many that would constitute misdemeanors or lower-level felonies in the West—are classified as "administrative violations" (行政违法). These are governed by parallel statutes, most notably the Public Security Administration Punishments Law (治安管理处罚法) and now the draft Cybercrime Prevention and Control Law. They are adjudicated directly by administrative organs, primarily the police, without prosecutorial review or a court trial. For a comprehensive academic analysis of this administrative-criminal divide and the expansive punitive powers of the Chinese police, see Sarah Biddulph, Legal Reform and Administrative Detention Powers in China (Cambridge University Press, 2007).

To read this article on the Jamestown website, click here.

Copies of the Apple Daily newspaper, published by Next Digital Ltd., move along a conveyor at the company's printing facility on June 18, 2021 in Hong Kong. (Source: Anthony Kwan/Getty Images)

White Paper Increases Securitization of Hong Kong

Eric Y.H. Lai
March 6, 2026

Executive Summary

- From the mainland's persepctive, Jimmy Lai's sentencing marked a significant moment for Hong Kong's security, as shown by the timing of the new White Paper's release. Past publications have aligned with legislation that tightened the mainland's grip over the Special Administrative Region (SAR).
- Beijing now recasts past Hong Kong political mobilizations as national security threats, even including those that were seen as legal under the Basic Law at the time, providing justification for its hardline turn.
- The new White Paper celebrates the Hong Kong government's use of polical, legislative, and educational initiatives to advance national security, and outlines new areas of focus, such as economic and international issues. This signals the possibility of mainland-style sanctions and renewed transnational repression efforts in the future.

On February 10, the State Council Information Office of the People's Republic of China (PRC) released a white paper titled "Realizing National Security Under 'One Country, Two Systems' in Hong Kong" ("一国两制"下香港维护国家安全的实践) (Xinhua, February 10). This marks the third white paper focused exclusively on the "one country, two systems" framework since President Xi Jinping took office. Previous documents were issued in 2014 and 2021, each responding to major institutional developments and subsequent political crises in the Special Administrative Region (SAR). Although the 2025 white paper on PRC national security referenced Hong Kong within a broader strategy, the 2026 document provides a more systematic and historically grounded articulation of Hong Kong's role in safeguarding PRC national security (Xinhua, May 12, 2025).

The 2026 white paper on Hong Kong articulates an official discourse designed to legitimize and rationalize the PRC's national security policies toward Hong Kong. It does so by providing a framework for localized political and ideological mobilization, and signals to local officials, pro-establishment actors, and Hong Kong society at large the strategic priorities and future direction of Beijing's governance approach.

Timing of White Papers is Symbolic

The timing of the 2026 white paper's release is significant. The first Hong Kong-focused white paper under Xi Jinping, titled "The Practice of the 'One Country, Two Systems' Policy in the Hong Kong Special Administrative Region," was released amid intensifying debate over universal suffrage (State Council Information Office [SCIO], June 10, 2014). Issued just 12 days before pro-democracy activists held an unofficial referendum as part of the "Occupy Central with Love and Peace" (和平佔中) campaign, the document was widely seen as a warning. It emphasized the central government's "overall jurisdiction" (全面管治权) and asserted that local administrators, including judges, must be loyal to the Party-state. In doing so, it redefined autonomy under "one country, two systems."

The second white paper, published in 2021, followed the first Legislative Council (LegCo) elections after Beijing overhauled Hong Kong's electoral system under the principle of "patriots administering Hong Kong" (爱国者治港) (SCIO, December 20, 2021) The redesigned framework effectively eliminated meaningful opposition participation through stringent political vetting. The 2021 document argued that the PRC—not the British colonial administration—had advanced Hong Kong's democratic development, that national security is a prerequisite for democracy, and that "anti-China" actors would be excluded from governance.

The 2026 white paper was released one day after media entrepreneur Jimmy Lai was sentenced to 20 years' imprisonment on national security charges (BBC News, February 9). Long portrayed by authorities as an "anti-China" figure with foreign ties, Lai is the only convicted individual explicitly cited in the white paper, underscoring his symbolic significance within the broader crackdown.

At nearly 19,000 Chinese characters, the 2026 white paper follows established narratives on "one country, two systems" and national security. It presents a state-centric historical justification for imposing the national security framework, outlines the central government's supervisory role, details Hong Kong's legislative and policy measures, reviews claimed achievements since 2020, and identifies future priorities for aligning Hong Kong society with the PRC's national security objectives.

Beijing Rewrites Hong Kong Narratives

The 2026 white paper endorses the narrative that

Hong Kong posed a national security threat to the PRC well before the 2019 anti-extradition movement. Under the emphatic section heading "An Unrelenting Fight for Safeguarding National Security in Hong Kong" (香港维护国家安全的斗争从未停止), the document asserts that the origins of this threat can be traced to resistance against the proposed Article 23 national security legislation in 2003 (Human Rights Watch, July 1, 2003; China Brief, July 15, 2003, July 29, 2003, March 1, 2024). From the Chinese Communist Party's (CCP) perspective, the failure to enact that legislation created structural vulnerabilities that enabled subsequent waves of mass mobilization. **[1]** The white paper links the 2003 setback to later protest movements, including the 2012 campaign against national education, the 2014 Umbrella Movement, the 2016 "Fish Ball" unrest, and the 2019 anti-extradition bill protests.

The inclusion of this narrative signals that mainland authorities now retrospectively characterize the 2003 mass mobilization—when more than 500,000 people protested the proposed Article 23 legislation—as a threat to national security. This reinterpretation stands in tension with the fact that the protests were widely regarded at the time as a lawful exercise of freedoms of expression and political participation protected under the Basic Law.

By framing the 2003 protests as security risks, the white paper recasts Hong Kong's long-standing democratization efforts and defense of civil liberties as destabilizing forces. Through this revisionist account of post-handover social movements, the document provides ideological justification for Beijing's hardline turn, which culminated in the imposition of the National Security Law in 2020.

Affirming Multi-Layered Security Governance

The 2026 white paper also articulates a new security governance structure in Hong Kong. The document reiterates that the central government bears ultimate responsibility for national security matters concerning Hong Kong, while the local government maintains jurisdiction over legislative, policy, and educational initiatives. However, it also promotes and celebrates alignment between central and local authorities.

The white paper asserts that the imposition of the National Security Law in 2020, together with the 2021 electoral overhaul, effectively suppressed destabilizing forces and restored stability. It also sees Hong Kong's legislation, judicial enforcement of security laws, and expanded national security education as strengthening security governance. Key milestones provided are the LegCo passing the Safeguarding National Security Ordinance in 2024 and the promulgation of two subsidiary pieces of legislation in 2025, the "Safeguarding National Security Regulation" and the "Safeguarding National Security Order" (GovHK, May 13, 2025). These last two instruments formally incorporated the operational authority of the Office for Safeguarding National Security (OSNS)—an agency directly accountable to the central government—into Hong Kong's domestic legal framework. **[2]** This development marked a significant step in embedding mainland security institutions within Hong Kong's legal system. It underscores that, rather than leaving security governance solely to the SAR under the rubric of "one country, two systems," the central authorities intend to retain a decisive—and increasingly operational—role in national security matters concerning Hong Kong.

The white paper further commends the Hong Kong government's approach to enforcing national security laws, adjudicating related cases, and expanding national security education.

Taken together, these elements suggest that legislation, law enforcement, judicial action, and ideological education will continue to function as a coordinated mechanism to ensure societal compliance with the national security framework (The Guardian, November 24, 2023).

Ongoing censorship and the criminalization of independent voices have reinforced this architecture. Judicial decisions imposing severe penalties on journalists for publishing materials deemed "seditious" have further narrowed the space for dissent (Reporters Without Borders, February 9). These developments collectively facilitate an environment in which the state can promote its national security directives and reshape historical narratives with limited bottom-up resistance.

Outlining New Battlefields for Safeguarding Regime Security

The white paper calls on the Hong Kong government to further strengthen coordination across both traditional and non-traditional domains of national security, encompassing internal and external dimensions. It also emphasizes the need to refine institutional arrangements and enforcement mechanisms in safeguarding national security. Within this forward-looking agenda, two new elements stand out.

First, the document signals an escalation in its approach toward opposition forces, extending the focus from domestic containment to action beyond Hong Kong's borders. The document says that "attention must remain focused on 'soft confrontation' under the slogans of 'democracy,' 'freedom,' and 'human rights,' and the reverse flow of agitator activities from overseas to Hong Kong must be closely monitored" (严防打着所谓"民主""自由""人权"口号的"软对抗"，严防海外反中乱港活动倒灌香港) (Xinhua, February 10). The link between so-called "soft confrontation" to the promotion of universal values effectively aligns Hong Kong's security governance with the mainland framework (Hong Kong Free Press [HKFP], June 30, 2025). This framing expands the scope of perceived risk from overt protest activity to ideological influence.

The document also signals heightened concern over cross-border information flows, particularly those connecting Hong Kong with overseas communities. Implicit in this language is growing attention to the expanding Hong Kong diaspora formed in recent years. Like other communities, segments of the Hong Kong diaspora—often in collaboration with Western political actors—have become increasingly vocal in criticizing Beijing's policies and countering the PRC's influence abroad.

This concern was evident in the aftermath of Jimmy Lai's sentencing, when several Western consulates in Hong Kong were summoned by the PRC's Ministry of Foreign Affairs office in the city and warned against "interfering" in local affairs. Since 2020, both the PRC and Hong Kong governments have invoked the extraterritorial provisions of national security legislation to target exiled activists and overseas organizations, reflecting an emerging pattern of transnational repression (The Atlantic Council, October 27, 2025). The white paper's call to forge "a broader united front at home and abroad" (更广泛 … 的统一战线) suggests that such outward-facing security measures may continue to expand. Transnational enforcement and influence strategies will be critical in the next phase of Hong Kong's security governance (BBC News, February 26; The Independent, March 4).

Second, the document suggests developing a robust approach to safeguarding non-traditional areas of security. These threats range from specific areas such as finance, shipping, and trade to the broader protection of overseas interests. For instance, the white paper

highlights the need to improve mechanisms for countering "foreign sanctions, intervention[s], and long-arm jurisdiction" (SCIO, February 10). This emphasis appears to respond, at least in part, to the recent controversy surrounding two Panama Canal ports previously operated by Hong Kong-based CK Hutchison. Amid rising geopolitical pressure from Washington, CK Hutchison reportedly sought to divest its port operations. Beijing, however, intervened and publicly criticized the proposed transaction, arguing that it could undermine PRC national security (The Guardian; RTHK, March 14, 2025). Geopolitical tensions between Panama, Hong Kong and the PRC further escalated as the Panama's supreme court annulled CK Hutchison's contracts. This allowed the firm to continue to operate the container ports, while the Panamanian government took control of them (BBC News, February 24). The episode underscores Beijing's growing sensitivity to the overseas commercial activities of Hong Kong-based enterprises. It suggests that the conduct of Hong Kong businesses abroad is increasingly viewed not merely as a commercial matter, but as an extension of Beijing's broader national security governance framework.

The PRC possesses several capabilities to improve mechanisms for countering such foreign threats. These could include expanding the extraterritorial application of Hong Kong's national security laws to cover foreign business entities, reviving efforts to introduce mainland-style anti-foreign sanctions legislation into the SAR, or enacting additional statutes to establish new enforcement bodies and further extend the security apparatus—similar to the expansion seen under the Critical Infrastructure (Computer Systems) Ordinance enacted last year (Xinhua, August 11, 2021; GovHK, January 1).

Regardless of the specific measures adopted, the trajectory is clear: Hong Kong's economic governance is increasingly being subordinated to national security priorities. Chief Executive John Lee has already announced plans to introduce a "Five-Year Plan" as Hong Kong's blueprint—an initiative that signals a gradual alignment of the city's traditionally market-driven model with the mainland's state-directed economic governance and development framework (HKFP, February 3).

Conclusion

Beyond its propagandistic function, the 2026 white paper makes clear that Hong Kong's "one country, two systems" framework is now firmly subordinated to the PRC's national security governance. As reflected in both the 2025 and 2026 white papers, the SAR is expected to function as a strategic node supporting the PRC's geopolitical objectives in the region and beyond.

The new document's strong emphasis on suppressing overseas opposition forces and ensuring that political power remains "in the hands of patriots" suggests persistent official anxiety about political control, both domestically and beyond Hong Kong's borders. Legal institutions are not merely neutral arbiters, but instruments to enforce this control. In practice, this risks further instrumentalizing Hong Kong's legal framework to facilitate censorship, constrain dissent, and monitor both political and economic actors within the city.

The white paper's deliberate reframing of Hong Kong's democratization movements and civil liberties struggles suggests that efforts to control historical memory will continue. By recasting past mobilizations as national security threats, the authorities lay the groundwork for sustained restrictions on freedom of expression and information flows. Further state-driven initiatives to promote an official narrative are likely, particularly as next year marks the 30th anniversary of the city's handover to the PRC.

Eric Y.H. Lai, *PhD is a Senior Fellow at the Center for Asian Law of Georgetown University Law Center, Washington D.C. He received PhD in Law at SOAS University of London. He was a visiting fellow at the Centre for Comparative and Public Law at the University of Hong Kong (2018–19), and a visiting researcher at the Dickson Poon School of Law, King's College London (2023). He has written more than 30 English commentaries, policy reports, and research articles on law, politics, and governance of Hong Kong and China. He is the author of Legal Resistance under Authoritarianism: The Struggle of the Rule of Law in Hong Kong (Amsterdam University Press, 2025).*

Notes

[1] Article 23 of the Hong Kong Basic Law would have required the regional government to enact its own laws prohibiting treason, secession, sedition, or subversion against the PRC, among other national security-related activities (basiclaw.gov.hk, accessed July 29, 2010). The bill failed to pass due to division in the pro-Beijing camp, but a version of it was ultimately enacted in 2024 under the Safeguarding National Security Ordinance (Hong Kong E-Legislation, July 11, 2024).

[2] Note that the promulgations were announced one day after the State Council released its 2025 white paper on PRC national security.

To read this article on the Jamestown website, click here.

"Internet of Things Town" in Hangzhou, Zhejiang Province, houses a cluster of digital technology companies focused on global business expansion. (Source: Sohu)

PRC Smart Television Risks and Ecosystem 'Enmeshment'

John Costello
February 27, 2026

Executive Summary

- Ecosystem enmeshment is transforming a bounded device-level risk into an open-ended one: smart television manufacturers in the People's Republic of China (PRC) are leveraging scale in commodity hardware to build durable control points across adjacent product categories, companion platforms, interoperability standards, and upstream component supply chains.
- Chinese smart television manufacturers retain privileged control over firmware, middleware, and over-the-air update pipelines, capabilities that could be leveraged for intelligence collection, behavioral modification, or network exploitation if engineers operating under PRC jurisdiction are directed or co-opted by state intelligence services.

Executive Summary (continued)

- Supply chain opacity—through joint ventures, original design manufacturing, and brand licensing—systematically obscures the identity of the firm exercising lifecycle authority over devices sold to U.S. consumers. This undermines every regulatory instrument that depends on identifying who controls what.
- The United States has no centralized federal authority establishing baseline cybersecurity or provenance requirements for consumer connected devices; existing tools govern transactions and specific entities, not the conditions under which firms sell into the domestic market. As enmeshment deepens, risks are compounding, while the window for early, lower-cost action narrows.

Editor's Note: This is the final installment in a five-part series exploring security risks associated with connected devices manufactured in the People's Republic of China. The previous four articles can be read here, here, here, and here.

In early February, the Chinese Communist Party (CCP) Central Committee and the State Council jointly released their first policy opinion of the year. Referred to commonly as "Document Number One" (一号文件), this document traditionally focuses on agriculture, rural areas, and farmers—a reminder of the Party's rural roots and supposed commitment to the masses (Xinhua, February 4). This year's was no different. But in a sign of the Party's growing push to diffuse advanced technology throughout the economy, the document's fourth section (out of 27) focused on "enhancing the effectiveness of agricultural science and technology innovation" (提升农业科技创新效能). For the first time, this section included a mention of the Internet of Things (IoT; 物联网) as a key part of pursuing new quality productive forces in the agricultural sector.

The inclusion of the Internet of Things in such an important policy document indicates the increasing prominence the Party is affording the technology as part of its desire to integrate digital interconnectivity into all aspects of society. This desire is not just confined to the Party's domestic ambitions, either. As recent Party media has noted, CCP General Secretary Xi Jinping has spoken about leveraging IoT as part of plans to "cultivate an independent, controllable, and continuously evolving platform ecosystem" (培育自主可控、持续进化的平台生态) overseas (People's Daily, February 12).

From a cybersecurity standpoint, the prospect of a global, connected, platform ecosystem that the government of the People's Republic of China (PRC) can control is concerning. But in many ways, it is already being realized. Smart televisions manufactured in the PRC provide a useful lens for understanding the potential scale of the problem. The technical architecture of these TVs, which includes the device stack, service models, data flows, and lifecycle control points, coupled with their increasing ecosystem enmeshment within the United States, creates a compounding set of risks that the U.S. governance system is not currently configured to confront.

The Compounding Risk

The risk posed by PRC-connected smart televisions is not a fixed quantity to be measured once and managed thereafter. It is a function of three interacting variables: original equipment manufacturer (OEM) leverage over firmware and update authority; the legibility of the supply chain to regulators and consumers; and the expansion of a bounded consumer product into an integrated ecosystem. These variables are mutually reinforcing. As the installed base grows, control over lifecycle updates persists, and branding detaches from technical authority. As a result, the television

assumes the characteristics of infrastructure, at which point the risk is no longer discrete, but compounding.

OEM Leverage: Capability Beyond Data Collection

Public debate centers on data collection, which is the visible surface of cybersecurity risk. But the more consequential issue is capability: what a manufacturer could do with its privileged position in firmware, middleware, and update authority if directed, pressured, or quietly co-opted by PRC state intelligence. This is the capability prong of the intent–access–capability framework introduced in Part 4, and it is where the service model distinctions outlined there become operationally significant (China Brief, February 20).

If the engineers who design and maintain firmware operate in PRC jurisdictions, they exist within a legal and political environment shaped by the 2017 National Intelligence Law (国家情报法) and the 2021 Data Security Law (数据安全法). Formal statutory obligation is only part of the picture. The informal capacity of the state to apply pressure, monitoring, and consequences without judicial process is more powerful. An engineer in Shenzhen or Qingdao does not need to be served with a court order to be co-opted. The organizational and political environment is itself the enforcement mechanism. [1] Every major PRC manufacturer examined in this series maintains its primary firmware and middleware engineering operations in the PRC mainland. U.S. offices exist—Hisense in Alpharetta, Georgia; TCL in Irvine, California; and Skyworth in Cypress, California—but none publicly discloses how many of its U.S. employees work on firmware, middleware, or telemetry code versus marketing, business development, and hardware sourcing. Where lifecycle software control resides inside the PRC system, structural exposure remains intact regardless of marketing footprint in the United States.

The manifestation of such exposure would not resemble a dramatic, easily discoverable backdoor. A more plausible construct is an intentional vulnerability embedded to appear as ordinary software error—a "bugdoor." **[2]** Firmware complexity provides natural camouflage. On a proprietary operating system like Hisense's VIDAA, the OEM controls the entire validation chain from bootloader through application layer, and there is no external audit layer. On a Google-certified Android TV build, the vendor partition is approved at certification time but not continuously monitored, and the depth of what Google actually inspects in an OEM's proprietary middleware is deal-specific and opaque. Attribution would be uncertain by design.

The decisive access point is the over-the-air (OTA) firmware update pipeline. The OEM generally controls signing authority, build systems, server infrastructure, rollout staging, and rollback policy. On Android TV, the OEM signs and hosts updates within Android's OTA mechanisms using OEM-controlled keys. Platform constraints limit arbitrary device takeover, but the capacity to modify behavior silently, post-sale, and at scale has few parallels in conventional intelligence collection. The critical unknowns—key custody, hosting location, update granularity, and rollback protections—are themselves risk multipliers. The less that is publicly documented about the update pipeline, the harder it is for external observers to assess whether it has been tampered with.

Capability does not require demonstrated exploitation to matter. It requires a structural position—and that position exists. Moreover, as the installed base expands, the leverage embedded in that pipeline expands with it.

Supply Chain Opacity: Who Controls What You Buy

Technical leverage deepens when the identity of the firm exercising it becomes obscured. Although firms do not disclose the distribution of their work

divisions, it is common across the industry for firmware authority, update control, and engineering to remain in PRC jurisdictions, while branding and retail presence appear Western-facing. Nothing at the point of sale indicates this to the buyer.

The pattern is well established. In January 2026, Sony and TCL announced plans to form a 51/49 joint venture to operate Sony's home entertainment business, covering the end-to-end chain from product development and design through manufacturing, sales, logistics, and customer service, with operations targeted for April 2027 (Sony Corporation; The Verge, January 20). Sony will retain its brand and proprietary image processing technology, but the device itself—hardware, firmware integration, and update pipeline—will be managed by the TCL-controlled entity. Senator Jim Banks (R-IN) raised national security concerns over the arrangement in February 2026. But as of this article's publication, no CFIUS review has been announced (U.S. Senate, February 2). In a separate example, Hisense acquired Sharp's North American TV operations in 2015 for $23.7 million, controlling the full device stack on Sharp-branded televisions for approximately four years before Sharp reclaimed the brand (EE Times, July 31, 2015). And as noted previously, the firm TongFang (同方), which is part-owned by the enterprise responsible for the PRC's civilian and military nuclear programs, manufactures televisions sold under the Westinghouse and Element brand names in the United States (CNBC, January 4, 2017; Consumer Reports, March 19, 2022; China Brief, February 20). Most recently, Skyworth has signed a deal with Panasonic to sell TVs to the North American and European markets (Sina, February 27). No consumer-facing indication of the device's provenance exists for any of these arrangements.

This is a governance-blinding problem. Any regulatory instrument, such as labeling, entity-list enforcement, ICTS review, that depends on identifying the firm responsible for firmware, update authority, or data routing is structurally undermined when brand identity is decoupled from technical control. The less legible control becomes, the harder it is to assess the scope of lifecycle authority embedded within the market.

From Device to Ecosystem

For now, platform partnerships with Google, Amazon, and Roku impose partial constraints on PRC manufacturers that mitigate some of the risks. Certification processes, app store governance, and operating system-level architecture limit unilateral OEM modification of certain layers of the stack. Automatic content recognition (ACR) data collection, while extensive, flows in most cases through U.S.-based advertising intermediaries rather than directly to PRC servers. At the regulatory level, attention is arriving, if belatedly, through consumer protection enforcement. As a result, the risk today is serious but not yet unconstrained. But the trajectory is integrative.

The growing expansion of PRC technology firms into the U.S. ecosystem could best be termed "ecosystem enmeshment." This phenomenon is a structural outcome of the intersection between PRC industrial-scale manufacturing policy and platform-mediated technology markets. The PRC's focus on cornering the market in consumer devices and IoT is far reaching. Scale in ostensibly commodity devices creates an installed base and a set of lifecycle control points —updates, apps, certifications, and service layers—that function as market infrastructure. Once embedded, that infrastructure lowers the barriers to entry into adjacent product categories and service layers, allowing low-margin penetration to translate into higher-leverage positions over time.

What begins as price competitiveness in commodity hardware becomes leverage over ecosystem architecture. Although enmeshment is not a coordinated conspiracy, it is the predictable byproduct of state-backed industrial scale combined with the economics of IoT and smart-device markets. Its cumulative effect is to create dependence as a byproduct of interoperability and convenience. Vendors with dominance in foundational consumer devices thus gain expanding influence across adjacent sectors, deeper into the stack, and across an increasing share of household and commercial environments.

This trend is visible in the smart TV sector, where devices are increasingly sold as part of an integrated smart home or app ecosystem. This transforms them from discrete data collection devices into something qualitatively different. Persistent behavioral monitoring infrastructure, when embedded in the household, becomes capable of capturing not just viewing preferences but security states, appliance usage patterns, environmental conditions, movement through the home, and network traffic across connected devices under the same control layer or within a potential lateral move.

Chinese manufacturers are actively pursuing this expansion strategy. TCL now offers robot vacuums, air purifiers, smart locks, and security cameras, all managed through the TCL Home app and controllable via the television as a household hub (TCL, accessed February 27). **[3]** Hisense's ConnectLife platform, meanwhile, integrates kitchen, laundry, air conditioning, and living room appliances under a unified control layer. At the technology trade show CES 2026, the company branded its strategy as a "full-scenario smart home ecosystem" (全场景智慧家庭生态) and announced expanded support for Google Home and Matter integration (LEDinside, January 8; Hisense, December 18, 2025). The deepening of stack position runs in parallel: Hisense has invested approximately $240 million to acquire a controlling stake in the Qingdao-based LED chipmaker Changelight to secure its display component supply chain (Yicai Global, February 1, 2023). Firms are also pursuing diversification beyond consumer electronics. Hisense's TransTech subsidiary provides AI-powered urban governance and traffic management systems; and both TCL and Hisense are entering automotive displays and semiconductor manufacturing (Hisense USA, December 18, 2024; OFweek, June 28, 2023). With expanding footprints across multiple sectors, these technology firms are compounding the governance challenge.

This challenge is further exacerbated by the ongoing disaggregation of responsibility for provenance. OEM licensing agreements, ODM arrangements, and white-label partnerships embed PRC-engineered software stacks in devices sold under other brands, attracting little public scrutiny even as the aggregate footprint expands. Companion apps aggregate data from across the ecosystem into single collection points. For instance, Hisense's ConnectLife app collects location, personal information, and usage data. TCL's Connect app does the same (Google Play, accessed February 27, [1], [2]). An adjacent challenge is that interoperability standards and cross-device coordination layers raise the cost of switching away from an ecosystem once a household is inside it. PRC state media have reported approvingly on this trajectory: Xinhua's coverage of CES 2025 emphasized Hisense's AI-powered innovations across display, smart home, and automotive domains (Xinhua, January 8, 2025). Its coverage of this year's event similarly highlighted PRC manufacturers demonstrating cross-device coordination and AI-driven automation across product categories (Xinhua English, January 10). The growth is largely silent, and it is accelerating.

The U.S. Response to Device Risk

Because this ecosystem expansion advances dynamically—through integrated platforms, interoperability standards, and white-label arrangements rather than discrete, legible transactions—it largely bypasses a U.S. regulatory apparatus designed to govern static products and identifiable firms. The tools available are oriented to discrete firms, identifiable transactions, and static product categories. Enmeshment, meanwhile, operates across categories, through iterative post-sale integration, and partially below the visibility threshold of any existing disclosure regime.

The Governance Void

The United States has no centralized federal authority establishing baseline cybersecurity requirements for consumer connected devices. Cybersecurity, consumer privacy, and digital device governance have never been designated as areas principally regulated by federal agencies—outside sector-specific cases such as healthcare, financial services, and telecommunications, they are left to the states. Every comprehensive federal privacy bill introduced to date has stalled in Congress (IAPP, accessed February 27). The statutes that are powerful in trade and commerce touch on the domestic device market only adjacently: CFIUS governs foreign acquisitions, the Entity List restricts exports, and the Federal Communications Commission's Covered List addresses telecommunications infrastructure. None sets market requirements for a set of firms offering a class of devices to U.S. consumers, and none addresses the embedded firmware and middleware risks at the device level. They govern transactions, not products. By late 2025, the Entity List had swelled to over 1,000 Chinese firms (Reuters, September 29, 2025). But no firm has been listed for the aggregate risk its consumer devices pose to the domestic digital ecosystem. The narrower tools that can directly address the domestic supply chain—the ICTS authorities under Executive Order 13873, federal procurement prohibitions such as NDAA Section 889, and CISA Binding Operational Directives—set requirements on when and how specific transactions or agencies may act, but they do not impose baseline conditions on firms or products as a condition of market access.

Consumer labeling has been the most frequently proposed market-shaping alternative. But while it might help to reduce supply chain opacity, it is the least effective at changing consumer behavior, as a 2025 study on the FCC's new Cyber Trust Mark has shown (ACM, April 2025). **[4]** This finding is consistent with the underlying economics: device security compromise is about national-level data aggregation and infrastructure vulnerability, not individually threatening events. Consumers discount abstract, impersonal risk because the cost of compromise falls on third parties—a negative externality in which neither the purchaser nor the manufacturer bears the consequences (Lawfare, April 7, 2025). Civil enforcement actions can change the interpretation of existing law, as the FTC's 2017 settlement with Vizio, the Texas Attorney General's 2026 agreement with Samsung show (FTC, February 6, 2017, FOX 7 Austin, February 26). But they do not create new law—they merely bind the parties to the agreement, and cannot manifest authority that does not already exist within a statute's bounds. Federal agencies require a legal predicate to compel disclosure of data practices or firmware provenance, and the complexity of the modern device stack outpaces any static disclosure regime.

A national security risk determination does not require demonstrated exploitation to be legally or practically useful. But absent the institutional capacity to identify the risk in the first place, even that authority goes unexercised. In this vacuum,

governance defaults to prohibition by exception. Specific firms or product categories are restricted once risk reaches national-security salience. The Kaspersky prohibition (June 2024), the ICTS final rule on connected vehicles (Federal Register, December 6, 2024), and the Huawei and ZTE equipment bans each address a specific firm or product category through targeted restriction rather than through baseline requirements applied to the broader class of devices or suppliers at issue. The structural vulnerability in this approach is that a problematic firm or device class can continue its penetration of the U.S. market relatively unchecked until its scale, impact, or visibility is sufficient to warrant national security attention —if it ever does. This model is reactive. It addresses visible manifestations of scale rather than the structural conditions that produced them.

Ecosystem enmeshment is antithetical to this approach, by providing few direct, targeted areas where risks and ecosystems are bounded enough to make prohibition enforceable and meaningful. As a result, the PRC's strategy of low-cost manufacturing, which leads to indispensability in commodity ICT devices and components, is translating into greater market power and deeper embedding in U.S. homes and infrastructure. This makes dependence on PRC-origin technology stacks unavoidable, difficult to identify, and costly to reverse. The logic is explicit in Chinese policy commentary, which emphasizes deep market integration and raises the cost of restriction to the restrictor (CCTV News App, October 16, 2024; Economic Herald, January 2, 2025). Targeted bans do not address such sweeping forces.

The Closing Window

Enmeshment alters the cost curve of intervention. When lifecycle authority is concentrated in a small installed base, regulatory action can operate at the level of firms or product lines. Once that authority is distributed across millions of devices, companion applications, interoperability standards, and adjacent product categories, disentanglement becomes a systemic challenge rather than a discrete one.

The telecommunications precedent illustrates the point. The FCC identified tens of thousands of pieces of Huawei and ZTE equipment across thousands of carrier locations in the United States, and Congress appropriated $1.9 billion for a reimbursement program (SDxCentral, February 11, 2022). But even with a finite and identifiable inventory of network equipment, removal proved underfunded and slow. The Commission has estimated that almost $5 billion is needed, and roughly 40 percent of recipients have reported they cannot complete replacement without additional funding (Reuters, May 2, 2024). While that case involved thousands of nodes, the consumer IoT ecosystem involves tens of millions —embedded in private homes, coupled to cross-device platforms, and integrated through shared applications. There is no equivalent of a rip-and-replace program for distributed household infrastructure. **[5]**

Enmeshment will make intervention harder over time, as identifying the scope of U.S. dependence on PRC-origin technology and addressing instances where that dependence proves unacceptable becomes increasingly difficult. As PRC vendors expand from televisions into smart-home devices, companion apps, and cross-device platforms, they deepen their footholds across an ever more diverse set of applications and market segments. All the while, U.S. regulatory tools remain oriented toward discrete transactions and firm-specific prohibitions, with no mechanism for continuous visibility into firmware provenance or update-chain control across an evolving ecosystem. The longer integration proceeds, the more expensive correction

becomes. Early action can operate at the level of market-entry conditions and transparency requirements. But late action requires prohibitions and large-scale unwinding. This kind of intervention, as seen in the telecom and social media cases, is disruptive and politically fraught. Once an ecosystem becomes infrastructural, policy no longer shapes its development—it reacts to consequences. The smart television ecosystem is at that inflection point now.

Conclusion

The combination of PRC state policy, organizational control through CCP institutional ties, and the technical capability assessed across the fourth and fifth parts of this series creates a system of risk, not a collection of isolated incidents. That system is compounding: OEM leverage deepens as installed bases grow, supply chain opacity thickens as joint ventures and ODM arrangements proliferate, and ecosystem enmeshment transforms a bounded device-level concern into an open-ended one.

The U.S. governance architecture, as presently configured, is structurally oriented to discover this problem late and address it expensively. But the window for governing the risk while it remains tractable has not yet closed. The smart television ecosystem is a live case study—and a preview of the challenge that will recur across every category of PRC-origin connected device entering American households. The way forward does not necessarily require total risk transparency or prescriptive regulation on the model of the EU's Cyber Resilience Act. But the current U.S. disposition is one of structural inertia, in which the aggregate risks of the devices Americans use are being shaped by Chinese industrial policy and a market that is largely blind, indifferent, or confused by its own dependence on PRC-origin technologies.

The United States will either develop the institutional capacity to see and shape ecosystem enmeshment while the market is still forming, or it will continue to inherit successive cases as late-stage prohibition. These will each prove costlier to impose, easier to retaliate against, and further from the underlying problem than the last. That choice has not yet been foreclosed, but the window in which it remains a choice is narrowing.

John Costello is a Senior Analyst for Cyber and East Asia at Flashpoint. He is a Cybersecurity Fellow for New America and former Congressional Innovation Fellow for the majority staff in the U.S. House of Representatives Committee on Oversight and Government Reform. John is also a U.S. Navy veteran and former NSA Analyst, and he is fluent in Mandarin Chinese.

Notes

[1] For a detailed treatment of the organizational and political mechanisms through which PRC state intelligence leverages technology companies, see Parts 1–3 of this series (China Brief, July 25, 2025, August 7, 2025, September 19, 2025).

[2] The term "bugdoor" refers to an intentional vulnerability embedded in code and designed to be indistinguishable from an accidental software bug. Unlike a traditional backdoor, which is a discrete, identifiable access mechanism, a bugdoor exploits the inherent complexity and imperfection of software to provide deniable access.

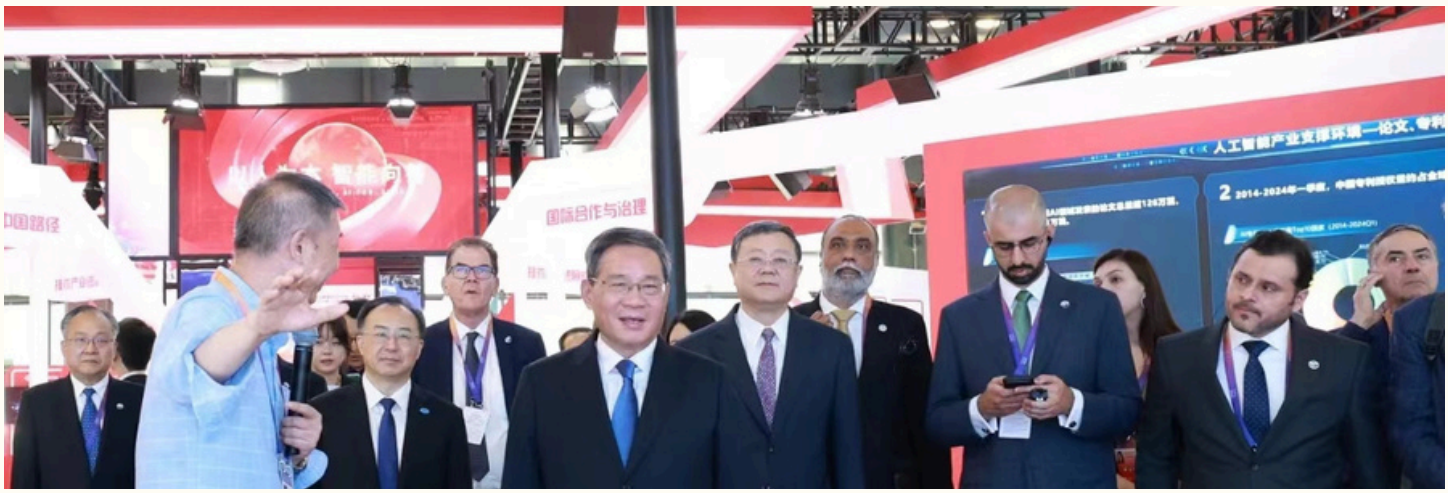
[3] As an aside, recent revelations that an individual was able to simultaneously access thousands of robot vacuum cleaners manufactured by another PRC firm, DJI, is only the latest example of the potential cybersecurity risks such ecosystem-integrated devices pose. In the DJI case, the individual was able to remotely

control the robovacs, look and listen through their live camera feeds, and even generate a complete 2D floor plan of device owners' homes (The Verge, February 14).

[4] Caven, Peter, Ambarish Gurjar, Zitao Zhang, Xinyao Ma, and L. Jean Camp. "Usability, Efficacy, and Acceptability of the U.S. Cyber Trust Mark." In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25), Article 1096, 1–35. New York: Association for Computing Machinery, 2025. https://doi.org/10.1145/3706598.3713463.

[5] TikTok illustrates the same dynamic at the application layer: enforcement was repeatedly delayed through 2025, and the eventual resolution required a complex ownership and governance structure rather than a clean prohibition (Reuters, January 23).

To read this article on the Jamestown website, click here.



Premier Li Qiang at the 2024 World AI Conference and High-level Meeting on Global AI Governance (Source: Xinhua)

PRC State-centric AI Governance Weakens Protection of Rights

Yaqiu Wang
March 6, 2026

Executive Summary

- The Chinese Communist Party's information control is embedded in Chinese AI models. As these systems are adopted globally, their built-in controls can be replicated at scale, entrenching Beijing-favored narratives and reasoning patterns in diverse information environments.
- The PRC promotes a global AI governance framework that foregrounds sovereignty, state control, and state-to-state cooperation, while giving limited attention to the role of nongovernmental actors and offering no commitments to rights such as access to information and freedom of expression. Wider adoption of this framework would weaken global protection of rights most impacted by AI.

Executive Summary (continued)

- The PRC's global AI governance approach should be read as part of the CCP's broader effort to shape international norms in ways that strengthen its grip on power at home and expand authoritarianism globally.

In February, U.S. artificial intelligence (AI) firm Anthropic alleged that three Chinese AI companies, DeepSeek, Moonshot AI, and MiniMax, had used large numbers of fraudulent accounts to carry out "industrial-scale" distillation attacks on its AI models, extracting outputs at volume to accelerate their own models' development (New York Times, February 23). Meanwhile, amid growing adoption of Chinese open-weight models in parts of the developing world, Washington has announced plans to send "Tech Corps" volunteers abroad to promote American AI models and support local adoption (Rest of World, February 20).

These developments reflect intensifying competition between the United States and the People's Republic of China (PRC) around AI, not just over capabilities and global model adoption, but also over what information controls and modes of governance will travel with these systems (China Brief, March 16, 2025, April 25, 2025). In the international arena, the PRC has consistently advanced a state-centric concept of governance that constrains individual rights. In the AI domain, the same conceptual emphases and omissions recur across PRC policy documents and intergovernmental cooperation agreements. Wider adoption of Chinese AI systems and Chinese AI governance model could entrench PRC government narratives and strengthen authoritarian governance practices internationally, and narrow the space to challenge them.

Information Control in Chinese AI and Its Global Export

Chinese AI models are gaining uptake in many parts of the world (Xinhua, February 14). In February, Chinese models accounted for over half of global token use—the first time this has been the case for a single month (21st Century Business Herald, March 2). Their appeal is based in part on cost, as they are comparatively inexpensive to deploy. This is an advantage in environments with compute and budget constraints. The most successful ones are open-weight models, which also lower barriers for local developers to fine-tune and deploy systems domestically without having to rely on foreign APIs. Broader digital cooperation initiatives under the PRC's Digital Silk Road initiative also facilitate uptake of these models. Chinese AI exports often come bundled as part of other deals. Telecommunications infrastructure built by Chinese companies—cloud services, data centers, 5G networks—provides a ready-made ecosystem for deploying Chinese AI systems.

Domestically, the PRC's AI governance model treats information control—referred to in the CCP's lexicon as "information guidance" (舆论导向)—as a core design requirement (China Media Project [CMP], February 9). The "Interim Measures for the Management of Generative AI Services (2023)," the country's primary regulation for generative AI, requires providers and users to "adhere to core socialist values" (社会主义核心价值观) and to prevent the generation of content that, among other things, "incites subversion of state power" (煽动颠覆国家政权), endangers national security and interests, damages the national image, or undermines national unity and social stability (Cyberspace Administration of China [CAC], July 13, 2023) In practice, this means that data the CCP deems politically sensitive must be excluded from training pipelines, and that models must be engineered with robust output filtering to block

prohibited content. This architecture is reinforced by broader national security and information control statutes, including the 2015 National Security Law and the 2017 Cybersecurity Law, which criminalize speech the state perceives could threaten the Party's monopoly on power (Baidu Baike/中华人民共和国国家安全法, accessed February 28, 2025; National People's Congress, December 29, 2025). **[1]**

A growing body of empirical testing suggests that leading Chinese large language models (LLMs) apply systemic restrictions and narrative steering on topics that the CCP views as politically sensitive. These models have been found to refuse answers, provide evasive responses, or reproduce state-aligned framings on issues such as Tiananmen, Xinjiang, Taiwan, and President Xi Jinping (NewsGuard, July 25, 2025).The extent of control moves beyond censoring information to shaping the contours of permitted knowledge, delimiting what is framed as controversial and what is presented as fact.

Three recent European assessments of Chinese AI models have found that leading models embed content controls that overreach the PRC's domestic political sensitivities, for instance by providing distorted information in relation to Russia's invasion of Ukraine (CEPA, February 27). A report by the China Media Project, meanwhile, found that a local-language chatbot in Uganda, built by fine-tuning Alibaba's Qwen-3 model, not only echoes Beijing's preferred narratives about the PRC, but also softens criticism of Uganda's own government (CMP, December 17, 2025).

When Chinese models are exported, their embedded information controls can be applied at scale. Even if a local developer fine-tunes a model for local use, the baseline "political security" configuration can remain intact. A separate China Media Project study shows that when a DeepSeek model was deployed internationally, some firms attempted to remove pro-CCP bias, sometimes unsuccessfully, while others did not bother (CMP, March 4, 2025).

Global AI Governance Proposals Foreground State-centric Approach

Internationally, the RPC promotes an AI governance framework that foregrounds sovereignty, state control, and state-to-state cooperation. This approach, which echoes Beijing's views in other domains, puts development and security at its core while giving limited attention to the role of nongovernmental actors and offering sparse commitments to protecting individual rights.

To date, the PRC has promulgated several high-level proposals on global AI governance. The most notable is the "Global AI Governance Initiative" (全球人工智能治理倡议). Introduced by President Xi Jinping in his speech at the 2023 Opening Ceremony of the Third Belt and Road Forum for International Cooperation, it calls for "respecting other countries' sovereignty, strictly abiding by their laws, and accepting their legal jurisdiction" (应尊重他国主权，严格遵守他国法律，接受他国法律管辖) (MFA, October 20, 2023). Beijing's Global AI Governance Action Plan, a 13-point framework released in 2025, calls for a UN-centered digital governance system based on "respecting national sovereignty" (尊重国家主权), and emphasizes support for developing countries to pursue AI "in line with their national conditions" (结合自身国情) (Xinhua, July 29, 2025). Although the action plan urges "actively safeguarding personal privacy and data security" (积极维护个人隐私和数据安全), it does not address rights central to information governance, such as access to information and freedom of expression.

This state-centric approach is also evident in bilateral and multilateral documents on AI cooperation.

Figure 1: Beijing's State-Centric Discourse in AI Policy Plans

Document	Release date	State-centric, counter-Western dominance language	Sources
AI Capacity-Building Action Plan for Good and for All (人工智能能力建设普惠计划)	Sept 2024	"On the basis of the principle of sovereign equality … through forms such as North-South cooperation, South-South Cooperation, and trilateral cooperation, efforts should be made to effectively implement the UN General Assembly resolution on strengthening international cooperation on AI capacity-building."	(MFA, September 27, 2024)
BRICS Leaders' Joint Statement on Global AI Governance (金砖国家领导人关于人工智能全球治理的声明)	Jul 2025	"Digital sovereignty and the right to development" is the "key" to global AI governance.	(BRICS, July 6, 2025)
Forum on China-Africa Cooperation—Beijing Action Plan (2025-2027) (中非合作论坛-北京行动计划（2025-2027）)	Sept 2025	"oppose ideology-based bloc confrontation, and safeguard the common interests of the Global South in the ongoing reform of global governance system…The African side adheres to the one-China principle and is ready to provide firm support to China on issues relating to its core interests and major concerns."	(MFA, September 5, 2025)

Figure 1 : Beijing's State-Centric Discourse in AI Policy Plans (continued)

Document	Release date	State-centric, counter-Western dominance language	Sources
Shanghai Cooperation Organization Leaders' Council Joint Communique (上海合作组织成员国元首理事会天津宣言)	Sept 2025	"All countries enjoy the equal right to AI development and adoption." (各国都享有平等发展和利用人工智能的权利)	(MFA, September 1, 2025)
"China's Plan for Global AI Governance: Building Together a Community with a Shared Future for Mankind in the Intelligent Age." An article by Consul General Luo Shixiong in Yekaterinburg (驻叶卡捷琳堡总领事罗世雄在俄媒体发表署名文章《全球人工智能治理中国方案：共筑智能时代人类命运共同体》)	Oct 2025	"AI should…advance technological progress through openness and cooperation and become a new bridge for building a community with a shared future for mankind. Some Western countries are using their advantages in technological monopolies to pursue unilateralism and technological hegemony, constructing a technological 'moat.'" （人工智能……应以开放合作推动技术进步，成为构建人类命运共同体的新桥梁。部分西方国家利用技术垄断优势推行单边主义和"技术霸权"，构建技术"护城河"。）	(PRC Consulate in Yekaterinburg, October 22, 2025)

Some of these do not just promote Chinese models but criticize Western models as proprietary and exclusionary, arguing that technology monopolies and restrictive supply chains entrench unequal access. This allows Beijing to promote "open" cooperation—especially among Global South partners—as both a development strategy and a geopolitical counterweight to perceived Western dominance. Table 1 below provides several illustrative examples of this language taken from various initiatives, plans, communiqués, and other official statements.

Rhetoric and Practice Diverge

A glaring problem in the PRC's vision for global AI governance is the gap between its rhetoric and its practice. Beijing regularly presents itself as a champion of "inclusive" and "fair" AI and warns against monopolies and exclusionary standards. Yet when international efforts are convened outside of its preferred frameworks, it has often been reluctant to endorse the resulting commitments. For instance, in September 2024, the PRC did not sign on to the Council of Europe's Framework Convention on AI, which aims to ensure that AI activities are consistent with human rights, democracy, and the rule of law. That same month, it also refused to endorse a blueprint for ethical, human-centric military AI use that was backed by dozens of countries at the Responsible AI in the Military Domain (REAIM) summit in Seoul in September 2024. At a subsequent REAIM summit held in Spain in early 2026, both the PRC and the United States opted out of a joint declaration (Reuters, February 5).

The contrast is even sharper when set against the PRC government's own conduct at home. The BRICS Leaders' Joint Statement on Global AI Governance, released in July 2025, called for respect for countries' linguistic, cultural, and ethnic diversity, and stressed the need to mitigate discrimination and bias in AI systems (BRICS Information Centre, July 6, 2025). A joint statement with France on AI and global governance similarly says that both countries "hold that AI must provide inclusive access for all, make content available in ways that … respect linguistic plurality and cultural diversity" (MFA, May 7, 2024). But the PRC's extensive use of data-driven and algorithmic systems to police and control minority communities—and to shape public narratives about the abuses—runs contrary to these stated principles. An Australia Strategic Policy Institute report finds that the country is using minority-language LLMs to deepen surveillance and control of ethnic minorities, both within the PRC and abroad (*Australian Strategic Policy Institute*, December 1, 2025). This comes as the National People's Congress in early March deliberates a law on "Promoting Ethnic Unity and Progress" (民族团结进步促进法), which seeks to erase minority language rights (Human Rights Watch, September 27, 2025).

Alignment with broader International Governance Strategy

Beijing's rhetoric may diverge from its practice, but its platitude-filled policy documents are not harmless. They are designed as part of a sustained, multipronged effort to normalize a state-centric model of governance. The emphasis on sovereignty, security, and development across its AI documents aligns with Beijing's broader vision for a new international order, which are embodied in Xi's four signature global initiatives, covering development, security, civilization, and governance (Qiushi, October 15, 2025; China's Diplomacy in the New Era, March 4).

The PRC approach to global AI governance also closely tracks the aim it has advanced for global Internet governance. Its digital diplomacy stresses that states should respect other states'

sovereignty and jurisdiction over data and that companies should abide by the laws of the country where they operate. These clauses normalize the view that cross-border digital services are governed first by state legal authority, not by international human rights standards or multi-stakeholder accountability (U.S.–China Economic and Security Review Commission, March 13, 2025).

It is also consistent with patterns documented in its engagement with the international human rights system: privileging state authority, limiting languages that strengthen civil and political rights protections, and narrowing the space for non-state actors, especially civil society (Brookings Institution, September 14, 2020; Journal of Democracy, July 2021; China Brief, February 6). **[2]** It has consistently advanced these objectives at the UN and other international fora by coordinating with "Global South" states and other authoritarian governments.

Conclusion

Beijing is systematically driving global adoption of Chinese AI models. These models are designed with information controls that ensure responses are titled in its favor. In parallel, the PRC is advancing an AI governance agenda that centers the state, marginalizes other stakeholders, and de-emphasizes rights such as access to information and freedom of expression. This posture is consistent with the country's broader efforts to reshape international norms in ways that strengthen its rule domestically and expand its influence globally. The long-term implication is a global information environment heavily shaped by Beijing, alongside AI governance norms that legitimize expansive governmental discretion over the protection of individual rights.

Yaqiu Wang is a fellow at the University of Chicago's Forum for Free Inquiry and Expression.

Notes

[1] An amendment to the Cybersecurity Law that came into force on January 1 contains, among other things, higher penalties for violating cybersecurity.

[2] Rana Siu Inboden, "China at the UN: Choking Civil Society," Journal of Democracy 32, no. 3 (July 2021): 124–35.

To read this article on the Jamestown website, click here.

Chinese state medea releases footage showing the Type 075 amphibious assault ship Hainan task group making its first appearance in PLA drills around Taiwan. (Source: USNI)

The Type 075's Operational Integration in Justice Mission-2025

Yu-cheng Chen & Yang Shang-wei
March 6, 2026

Executive Summary

- In late December 2025, the PLA Eastern Theater Command launched the Taiwan-focused joint exercise "Justice Mission-2025." Officially released training items included "blockade and control of key ports and areas" and "outer-line three-dimensional deterrence," while Chinese reporting suggested the presence of a Type 075 amphibious assault ship—making the platform a key entry point for assessing the PLA's evolving outer-line intervention-denial concept.
- Rather than implying that aircraft carriers will disappear from Taiwan contingencies, the forward positioning of a Type 075 task group in this exercise suggests the PLA is experimenting with alternative large combat platforms for "outer-line" employment.
- The Type 075's activity pattern also suggests a "far-seas mission first, Taiwan exercise second" logic—consistent with PLA emphasis on using one deployment for multiple objectives, while highlighting the growing centrality of ASW capacity to any future attempt to contain Taiwan and deter external forces.

In late December 2025, the Eastern Theater Command of the People's Liberation Army (PLA) announced a military exercise titled "Justice Mission 2025" (正义使命—2025). The announcement explicitly highlighted "blockade and control of key ports and areas" (要港要域封控) alongside "outer-line three-dimensional deterrence" (外线立体慑阻) (China Military Online, December 30, 2025; China Brief, January 9). This emphasis indicates that Beijing is now framing exercises around Taiwan more openly as aimed at preventing external intervention, and not just conducting near-shore operations.

State media reporting in the People's Republic of China (PRC) further referenced activity associated with a "Type 075" (075型) amphibious assault ship—a form of large helicopter platform. This was the first time a Type 075 formation has featured prominently in coverage of an Eastern Theater Command drill centered on Taiwan, highlighting the platform's emerging role, though it does not does not entail that the exercise's primary training theme was amphibious assault (Global Times, December 29, 2025).

"Justice Mission-2025" followed a year in which official narratives around the PLA's Taiwan-related exercises increasingly stressed integrated inner-line and outer-line linkage and multi-axis containment. For example, during the first "Joint Sword" (联合利剑) exercise in April 2023, reporting indicated that the Shandong carrier group operated east of Taiwan, establishing an outer-line pressure precedent (Global Times, April 11, 2023; China Brief, May 5, 2023). In PLA operational discourse, the "inner line" generally refers to operations conducted in the PRC's near seas and around Taiwan and the Taiwan Strait, while the "outer line" refers to operations or forces positioned east of Taiwan and along the approaches from the Philippine Sea, intended to deter or delay external intervention.

From Carrier 'Outer-Line Presence' to Type 075 'Outer-Line Deterrence'

In recent Taiwan-focused drills and exercises, the aircraft carrier has typically been the PLA Navy's most visible outer-line platform east of Taiwan. Carriers are a conspicuous signal of far-seas sortie generation, fixed-wings flight operations, and send a political message that external forces would face escalation risk if they attempt to intervene. This pattern is evident in recent large-scale activities. The Shandong was linked to Joint Sword (2023), the Liaoning was associated with Joint Sword-2024B, and the Shandong also appeared in Strait Thunder-2025A (Eastern Theater Command [ETC] Weibo, April 10, 2023; ETC, October 14, 2024; CNA, April 2, 2025).

Against this backdrop, the emergence of a Type 075 task group in December 2025 represents a notable shift. Rather than emphasizing the carrier as its signature outer-line platform in these exercises, the PLA highlighted a large-deck amphibious ship with different operational strengths. This shift aligns with PLA strategic thinking on the Pacific theater. The PLA views the Pacific direction as central to achieving "military presence" (军事存在) beyond the first island chain, reshaping the maritime balance in the Western Pacific, and using the outer line to deter or harass U.S. and Japanese forces with the aim of delaying interference in the PRC's near seas (the inner line) (INDSR, December 8, 2025).

"Justice Mission-2025" also points toward a more layered, composite approach. Chinese reporting stated that the amphibious assault ship formation operated in the Philippine Sea, training items such as ship–aircraft coordination, near- and far-seas strike, and integrated support—activities that are consistent with building a more persistent and flexible outer-line deterrence posture (Xinhua, December 30, 2025). At the same time, the

publicly described formation did not resemble a classic amphibious assault rehearsal package. The absence of commonly paired platforms in an amphibious "delivery-type" configuration—especially dock landing ships and other landing vessels—makes it difficult to interpret the exercise as primarily built around large-scale ship-to-shore landing or "vertical envelopment" as the core objective.

Task-Group Logic: Far-Seas Training First, Taiwan Exercise Second

Over the past several years, PLA Navy far-seas activity has evolved from single-ship transits to diverse, realistic, and highly integrated task-group operations. These have increasingly been characterized by far-seas combat training, island chain transits, and normalized presence.

Chinese doctrinal and educational writings describe naval development under the strategic requirement of "near-seas defense, far-seas protection" (近海防御、远海护卫). This refers to accelerating toward greater platform size, systemization, compositing/integration, and unmanned capabilities, while improving strategic deterrence and counterstrike, far-seas maneuver operations, near-seas combined operations, comprehensive sea-area control, amphibious operations, and integrated maritime support. **[1]**

Research from the PLA Navy's Dalian Naval Academy suggests that, partly informed by U.S. Amphibious Ready Group (ARG) experience, the PLA groups Type 075 formations into two broad categories— "lean" and "delivery"—for missions such as far-seas combat patrols and emergency contingency response:

- "Lean" formation (1+2): one Type 075 plus 1–2 escorts (destroyers/frigates), optimized for flexible far-seas patrol, contingency response, overseas presence, special operations forces carriage, and limited equipment packages.
- Delivery" formation (1+2+3): one Type 075 plus 1–2 amphibious landing platforms ("LPDs") and 2–3 escorts (destroyers/frigates), emphasizing larger-scale troop delivery and battalion-sized air-assault and amphibious assault forces (see Figure 1).

Figure 1: Type 075 Task-Group Categories and Mission Patterns

Formation Type	Composition	Primary Mission Objectives	Operational Characteristics
Lean Model (精幹型)	1 + 2(1 Type 075 + 1-2 escorts)	Far-seas combat patrols, emergency response, counter-terrorism, and Non-War Military Operations (NWMO)	Emphasizes rapid response and low-cost presence; ideal for protecting overseas interests and patrolling specific maritime corridors.
Delivery Model (投送型)	1 + 2 + 3 (1 LHD + 1-2 LPDs + 2-3 escorts)	Large-scale power projection, multi-dimensional landing operations, and seizure of key ports or territories.	Focuses on integrated systemic combat; possesses the capability to project heavy combined-arms battalions for high-intensity amphibious conflicts.

(Source: Chengyi Yin [尹成義], "Research on Optimizing Amphibious Assault Ship Formation Composition Models and Decision Models"[兩棲攻擊艦編隊組成模式與決策模型優化研究], Fire Control and Command Control [火力與指揮控制] 47, no. 7 (July 2022): 63-64.)

The recent deployment timeline of Type 075 vessels reinforces this interpretation. Reporting indicates that a task group including the Type 075 (Hainan) and a Type 055 surface combatant was detected north of Palau as early as December 5, 2025, suggesting a far-seas operating radius and mission set not limited to Taiwan (USNI News, December 5, 2025).

Placing "Justice Mission-2025" into the broader context of far-seas activities in 2025, the Type 075 appears more likely to have operated first as part of a far-seas task group, before being folded into a Taiwan exercise framing. This would be consistent with PLA practice and discourse, which emphasizes "one action, multiple missions" (一次行动兼容多类任务). PLA educational materials describe this as "killing two birds with one stone" ("一箭双雕"). **[2]**

Treating the Type 075's appearance in "Justice Mission-2025" as proof that the PLA's primary training objective was amphibious assault therefore likely overestimates the "delivery-type" landing component of the exercise. A more conservative and analytically useful interpretation is that the Type 075 formation served outer-line denial/interdiction needs east of Taiwan.

Anti-Submarine Warfare at Core of Strategy East of Taiwan

The PLA's operational aim has remained consistent across Taiwan-focused exercises, whether it has deployed an aircraft carrier or a Type 075 task group east of Taiwan. That aim has been to provide an outer-line presence intended to disrupt Taiwan's external connections and complicate external reinforcement. State media described "Justice Mission-2025" training as including joint formations operating in Taiwan's north, east, and southwest areas, with items such as joint anti-submarine warfare (ASW) and maritime strike, as well as coordination with the Type 075 Hainan formation to validate inner-line and outer-line linkage (CCTV, December 29, 2025).

If the PRC were to attempt containment or blockade-like pressure against Taiwan, ASW would become indispensable, particularly because the most consequential uncertainty in an intervention scenario is the entry of external attack submarines, including nuclear-powered submarines, into the waters east of Taiwan. In such a scenario, undersea forces could impose outsized risk on PLA surface task groups attempting to sustain outer-line presence. Consistent with this logic, U.S. assessments and comparative analyses often regard PLA Navy ASW as a persistent challenge, while treating U.S. undersea warfare as a relative advantage in far-seas operations (T2COM G2, December 6, 2024).

Chinese research indicates that the PLA is working to operationalize ASW as a calculable task rather than a conceptual aspiration. In a 2024 paper on optimizing ASW defensive formations during amphibious task-group transits published in the journal Command Control and Simulation (指揮控制與仿真), the researcher Chengyi Yin (尹成義) treats "amphibious platform survivability" and "task-group ASW" as a modeling and optimization problem, suggesting a drive to systematize tactics and formation design. **[3]** Other parts of the PLA research ecosystem discuss extending maritime containment through human-machine teaming and unmanned autonomy, implying that outer-line denial may increasingly include lower-visibility undersea control through unmanned underwater vehicles and distributed sensing. **[4]**

This trend connects to PLA platform modernization. The PRC Ministry of National Defense (MND) framed the Type 076 amphibious assault ship "Sichuan" in a recent press briefing

as an important platform to enhancefar-seas combat capability, signaling that amphibious aviation platforms are being institutionalized as part of the navy's broader transformation (MND, November 27, 2025). These comments form part of a parallel agenda in which the PRC displays new equipment in order to raise the risk and cost for other states considering intervention in a Taiwan contingency. For instance, Chinese analysis linked some of the systems showcased in the September 3, 2025 parade to reconnaissance and blockade tasks in key maritime corridors, implying that Beijing is building an operational concept to compete with the U.S. idea of turning the Taiwan Strait into a "hellscape," but with Chinese characteristics emphasizing corridor control, blockade options, and layered denial (Prospect Foundation, October 8, 2025). In this context, a Type 075's outer-line presence—especially if it enables higher-tempo helicopter operations and ASW-related training—should be interpreted primarily as a mission-driven capability rehearsal aimed at shoring up a far-seas shortfall while embedding ASW into a broader strategy of containment.

Conclusion

For Taiwan, the Type 075 amphibious assault ship remains a major security threat. But the training emphases highlighted in "Justice Mission-2025" and the overall operational pattern of the Type 075 task group in the Western Pacific earlier in the year, indicate that its core role in this context is not amphibious assault but as part of a broader effort to push Taiwan-related military pressure toward a layered framework of inner-line containment plus outer-line denial.

At the same, time, the decision to send a Type 075 task group forward in the most recent drills represents a departure from previous activities, in which aircraft carriers were the most visible platform east of Taiwan. This indicates that the PLA is experimenting with outer-line employment using different large combat platforms. By leveraging the amphibious assault ship's sustained helicopter operations, integrated support functions, and multi-mission composite characteristics, the PLA can generate an alternative, more durable model of outer-line presence and denial—one that is complementary to, rather than a replacement for, carrier operations.

More importantly, the Type 075 formation's timeline and order-of-battle logic point to a far-seas mission first, Taiwan exercise second pattern. By reframing an already deployed far-seas group within a Taiwan-focused drill narrative, the PLA can simultaneously reduce marginal deployment costs while achieving multiple objectives. This complicates partner warning indicators and makes it harder to interpret intent based solely on whether an activity is labeled a "Taiwan drill."

Operationally, the most consequential implication centers on ASW-oriented containment east of Taiwan. If external undersea forces constitute the largest uncertainty in an intervention scenario, the PLA must treat ASW as a core enabling condition for outer-line denial. The Type 075, as a large helicopter platform, can serve as a node for sustained aviation operations and maritime control, while also functioning as a mechanism for mission-driven "catch-up" in a domain where the PLA perceives persistent gaps. As Type 076 and unmanned/undersea systems mature, outer-line deterrence may increasingly evolve into more comprehensive multi-domain containment rehearsal aimed at strengthening the integrity and durability of a future blockade chain.

The views expressed are solely those of the authors and do not represent the positions of the National Defense University, the Ministry of National Defense, or the government of ROC (Taiwan).

Yu-cheng Chen is an associate professor at the Graduate Institute of China Military Affairs Studies, Fu Hsing Kang (FHK) College, National Defense University (Taiwan). He is also a member of the Research Project on China's Defense Affairs (RCDA). His research interests include the PRC's political warfare, PLA maritime power, and East Asian security. He received a scholarship for "Overseas Academic Diplomacy Program 2020 and 2023" from the Ministry of Foreign Affairs, Taiwan.

Yang Shang-wei is a graduate student at National Defense University. He previously served as the Combat System Officer (CSO) aboard a Cheng Kung-class frigate, a first-class vessel in the Republic of China (Taiwan) Navy.

Notes

[1] Chengyi Yin [尹成義], "Research on Optimizing Amphibious Assault Ship Formation Composition Models and Decision Models" [兩棲攻擊艦編隊組成模式與決策模型優化研究], Fire Control and Command Control [火力與指揮控制] 47, no. 7 (July 2022): 63–64.

[2] Tianliang Xiao [肖天亮], ed., The Science of Military Strategy [戰略學] (Beijing: National Defense University Press, 2020), 322–23.

[3] Chengyi Yin [尹成義], "Research on Optimizing Anti-Submarine Defense Formation Configuration for Amphibious Assault Ship Formations During Maritime Transit" [兩棲攻擊艦編隊海上航渡對潛防禦對形優化配置研究], Command Control and Simulation [指揮控制與仿真] 46, no. 2 (April 2024): 157–60.

[4] Fei Luo [羅飛], "Trends in the Evolution of Future Naval Warfare Forms and Their Implications" [未來海戰形態演進趨勢與啟示], National Defense Science and Technology [國防科技] 45, no. 3 (June 2024): 33–35.

To read this article on the Jamestown website, click here.

The 2026 Spring Festival Gala show hosted by China Media Group. (Source: Nanfang Daily)

Spring Festival Gala Centers High-Tech Again

Linda Zhang
March 6, 2026

Executive Summary

- The content of the annual Spring Festival Gala broadcast is useful for gauging the priorities of the ruling Chinese Communist Party for the upcoming year.
- Technological developments in artificial intelligence (AI) and robotics featured prominently in this year's program, with performances by humanoid robots and comedic sketches that touted technology as a potential solution to the PRC's social and demographic issues.
- Military parades, typically a part of the show, received less attention this year, potentially signaling the Party's desire to focus on issues such as innovation and promoting domestic consumption levels.

Every year, hundreds of millions of Chinese families gather together to celebrate the Lunar New Year. For many, an obligatory part of the festivities is the Spring Festival Gala (春晚), hosted and broadcast by China Media Group, the main state media corporation in the People's Republic of China (PRC). This year's spectacle lasted over four hours, featuring 49 segments of singing, dancing, comedic sketches, and other performances (Xinhua, February 16). The gala is a carefully planned and choreographed event. In addition to its entertainment value, it is engineered to highlight the government's accomplishments in the past year and share the Chinese Communist Party's (CCP) priorities with the country's 1.4 billion citizens, as well as the millions of Chinese people overseas.

Technology was the main theme this year. This comes as no surprise, as central government policy over the past 12 months has emphasized technological development and the adoption and diffusion of artificial intelligence (AI) across the country (China Brief, September 21, 2025, November 3, 2025).

High-Tech Takes Center-Stage

AI adoption and diffusion was evident throughout the program. It even found its way into comedy sketches. Combining short sketches (小品) and crosstalk (相声), one segment made fun of a young couple for being excessively glued to their phones and highlighted how AI algorithms could influence their relationship. Beyond comedy, AI was advertised extensively throughout the show to the hundreds of millions of live viewers. Doubao (豆包), ByteDance's (字节跳动) AI assistant, was the "AI partner" of the evening, and "assisted" the announcers in between performances. When they downloaded the application onto their smartphones, viewers at home were offered raffle prizes such as robots made by top robotics firm Unitree and drones made by flagship drone manufacturer DJI (South China Morning Post, February 11). Doubao reported over 1.9 billion user interactions during the broadcast—an order of magnitude more than the number of viewers for commercials advertising U.S. AI companies during the Superbowl the previous week (Caixin, February 18).

The year 2025 was the first in which the central government's work plan included a reference to embodied AI. State media explicitly linked this prominence to humanoid robotics performances during this year's gala, which were framed as a "window [on]to China's industr[ial] policies" (CGTN, February 17). This was not the first robotics performance at a Lunar New Year gala, which has become a custom in the last decade. For instance, last year's included a northern Chinese dance. But this year's was the most technically impressive to date. During a martial arts display in which robots performed a choreographed fight against human martial artists, the robots could be seen executing stunts, such as a backflip off a wall. The evolution of the gala's robotics sketches also provide insights into Chinese peoples' changing views about the role of technology in their lives and how they are reacting and adapting to government priorities. For example, in another comedy sketch, a grandmother criticized her grandson for not visiting her, instead professing a preference for her humanoid robot "grandsons" that had been taking care of her in his place. This lighthearted segment subtly engaged with traditional social customs, while also signaling awareness of social and demographic issues that the country is currently grappling with.

Besides technology and AI, the gala also hit other national priorities, including manufacturing. Gala organizers chose to highlight Yiwu, a county-level city in Zhejiang province best known for its manufacturing and e-commerce sectors. The announcers touted key manufacturing statistics and encouraged viewers to go out and spend more, in line with the government incentives

issued at the New Year to lift consumption levels (Xinhua, February 12).

Longstanding Gala Segments Receive Less Attention

Each year, the gala includes a military segment. This year was no different, featuring a section that was army-heavy and featured People's Liberation Army (PLA) Army soldiers stationed in Qinghai Province. The troops assured the audience that the frontier was well-defended and that people would not have to worry about their own safety. But aside from this obligatory PLA song segment and a small clip of the September 2025 military parade, military strength was not in the foreground, providing no indication that the CCP is preparing its population for war. Perhaps this is due to a desire to emphasize other priorities. But it could also reflect a need to minimize attention on an organization that has been beset with corruption scandals in recent months (China Brief, January 26). The country's space program, meanwhile, which has been featured in performances and transition segments in recent years, was omitted from the event altogether.

Other segments touched on a range of themes that the Party views as important. Agriculture and food security, for instance, were celebrated by touting the biggest grain harvest on record (Global Times, January 22). Ethnic unity, another common theme, was demonstrated with a children's fashion show. Children from each of the country's official 55 ethnic minority groups catwalked down a runway in their respective culture's traditional clothes—a common way in which official media tends to portray minority cultures. Traditional culture was also celebrated in the form of Peking opera, traditional instruments like the pipa, historic calligraphy, and Han dynasty statues of horses.

The Gala closes every year with the song "Tonight is Unforgettable" (难忘今宵), but this year's performance featured a new arrangement with stronger pop music elements.

Perhaps the biggest surprise of the night was an appearance by John Legend, who sang his 2013 hit "All of Me," as well as a Disney theme song with French singer Hélène Rollès. This was the second year in a row that an American artist participated in the Gala, as it seeks to draw in a wider international audience and attempts to signal the country's openness in the upcoming year.

Conclusion

This content of the 2026 Spring Festival Gala indicated that national leaders are in an ebullient mood when it comes to the country's advances in AI and robotics. After years of investment, these industries took center stage, as the PRC continues to portray itself as at the cutting edge of modernity. The annual event is a useful signal for gauging the national mood and policy priorities, even if it is not an explicitly political event. This year's affair held few surprises, but it indicated that observers should expect more of the same in the coming year in terms of economic priorities: more promotion of AI, more commercialization of robotics, and continued efforts to promote domestic consumption and drive exports.

Linda Zhang is a China Analyst at the RAND Corporation. She graduated from Johns Hopkins SAIS.

To read this article on the Jamestown website, click here.

The Jamestown Foundation is an independent, nonpartisan organization supported by tax-deductible contributions from corporations, foundations and individuals. To donate to Jamestown, please call (202)483-8888 or donate through our website: **www.jamestown.org**

A: 1310 L Street, NW, Suite 810,
Washington DC 20005
T: (202) 483-8888
F: 202 483-8377
W: jamestown.org