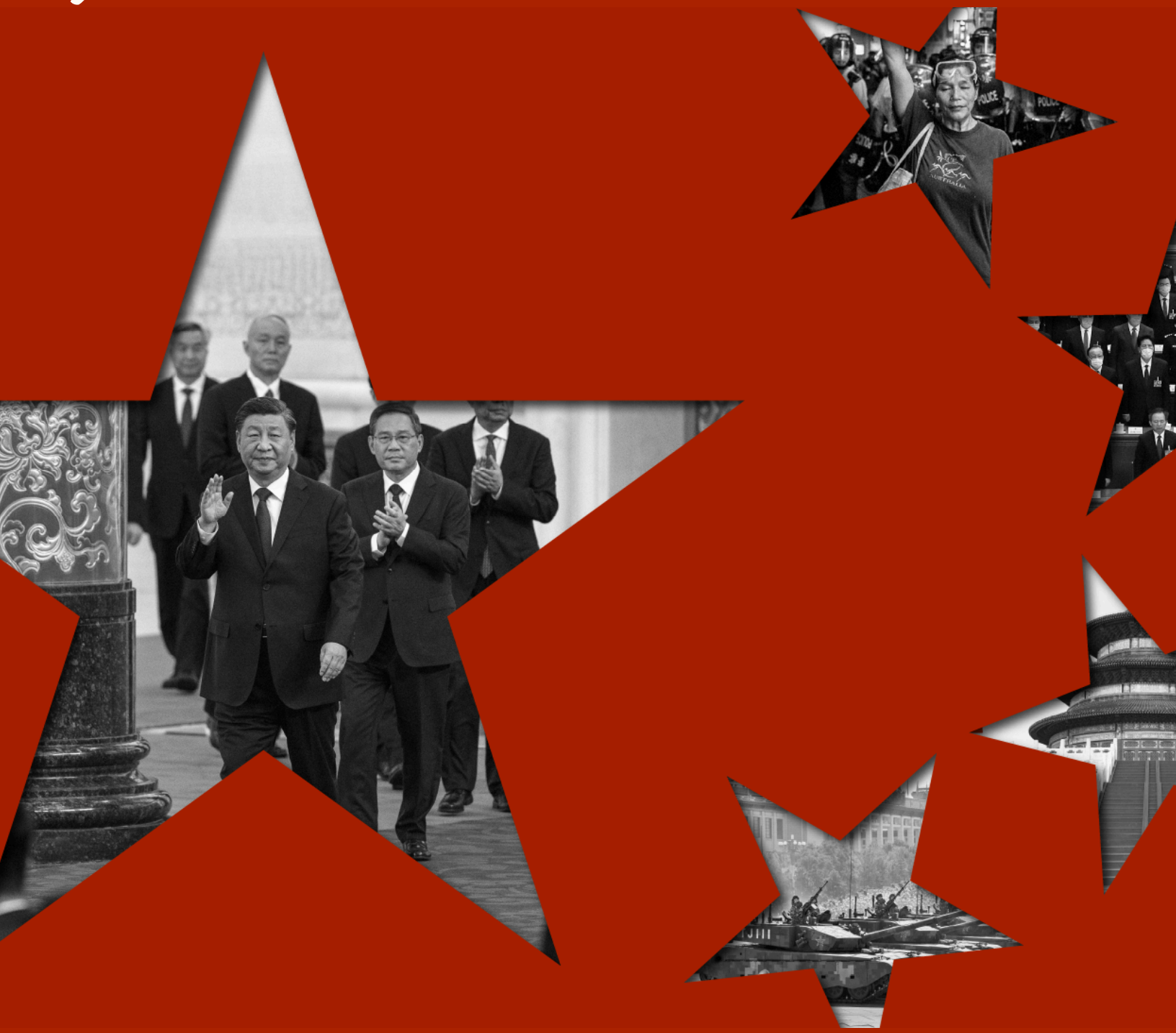
Jamestown

February 22, 2026



China Brief

Volume 26, Issue 4

In This Issue

China Brief

Information Warfare **3**
Recent ILD Activity Suggests Expanded Mandate
Jonah Reisboard

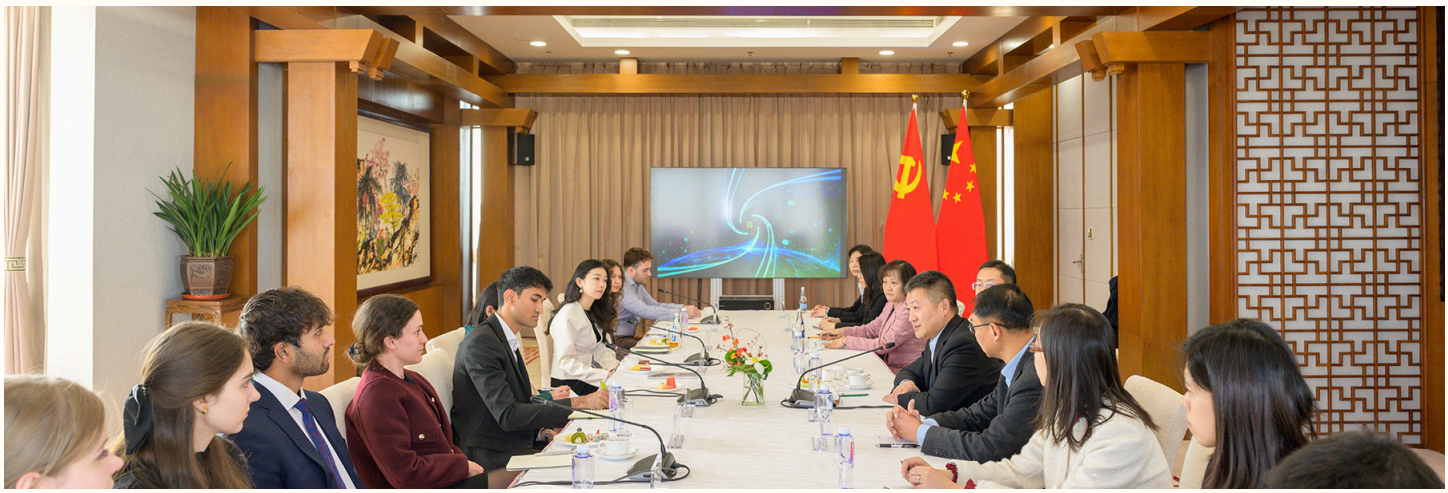
Economics & Energy **10**
The Low-Altitude Economy's Great Leap Upward
Youlun Nie

Military & Security **16**
PLA Reorganizes Space Information Support and Assurance Mission
Kristin Burke

Technology **23**
Technical Analysis Reveals Connected Smart TV Security Risks
John Costello

Notes

Military & Security **32**
Defense Minister Dong Jun Leading Contender for CMC Seat
Brandon Tran and Gerui Zhang



Students affiliated with the China–U.S. Exchange Foundation meet with representatives of the International Liaison Department (ILD). (Source: ILD, January 6)

Recent ILD Activity Suggests Expanded Mandate

Jonah Reisboard
February 17, 2026

Executive Summary

- The Party's International Liaison Department (ILD) has started conducting outreach to U.S. student groups—especially those at policy schools at elite universities—signaling an expansion of its mandate.
- Past changes to the ILD's mandate have been the result of insecurity, but current developments arose from internal perceptions of the People's Republic of China's (PRC) increasing national status in the 2010s.
- U.S. institutions that facilitate the ILD's youth outreach are misreading the department's intentions, as it now prioritizes promoting PRC global leadership over genuine political exchange.

In early January, the China–U.S. Exchange Foundation (CUSEF; 太平洋国际交流基金会), a Beijing-based non-profit, organized a trip to the People's Republic of China (PRC), bringing U.S. college students to Beijing, Guiyang, and Chengdu (CUSEF (Beijing), January 14). In Beijing, the students met with Lu Kang (陆慷), the vice minister of the International Liaison Department (ILD) of the Chinese Communist Party (CCP) (中共中央对外联络部) (ILD, January 6). The meeting was celebrated as part of Xi Jinping's "50,000 in 5 years" (五年五万) initiative, which follows his 2023 announcement that the PRC will encourage 50,000 young Americans to visit the country through exchange and study programs between 2023–2028 (Embassy of the PRC in the United States, December 7, 2024).

Visits to the ILD are rare. The department has hosted only six public meetings with U.S. students, all since 2024. In addition to the January meeting facilitated by CUSEF, meetings have included delegations from the University of Pennsylvania, Columbia University, Johns Hopkins University, and Harvard University (see Table 1).

The ILD's participation in the "50,000 in 5 years" initiative reflects a growing mandate. Described as the "CCP's 'ministry of foreign affairs'" (中国共产党的"外交部"), its scope of work traditionally covered promoting party-to-party relations and sharing the CCP's models of governance and development with receptive institutions, along with other auxiliary foreign policy functions (Hoover, 2019). These efforts have primarily been intended to expand the CCP's "circle of friends" (朋友圈), but recent youth visits show a new method of outreach (The Paper, June 27, 2016). The ILD now employs a grassroots approach that bypasses political points of contact, suggesting a more assertive approach to international influence.

From 'Demystification' to Student Outreach

Student engagement with the ILD is the most recent component of the department's "Enter the ILD" (走进中联部) program. The program was first introduced in 2007 with an ILD "Open Day" (开放日). Although held in the period's "spirit of openness" (开放的精神) as a means to "demystify" (去神秘化) the department, the day's events were only attended by representatives of Chinese institutions (China Online; Voice of America, September 25, 2007). The next iteration included foreign media, as did subsequent events (The Paper, June 27, 2016). In April 2011, foreign journalists witnessed a meeting between the ILD and a German cross-party parliamentary delegation; in June 2011 they watched talks between the CCP and the Mozambique Liberation Front; and a 2016 event featured a public discussion between the ILD minister and First Secretary of the Communist Party of Cuba Raúl Castro (China Daily, April 11, 2011; Xinhua, June 10, 2011; The Paper, June 27, 2016).

Previous "Enter the ILD" events purposefully exposed what the department is and how it works. Although some aspects remained choreographed, from 2007 into the 2010s, the ILD was working to be understood by the country and the world. Its leadership shared data on the CCP's links to political parties around the world and answered questions from foreign reporters on Party ties with counterparts in the Democratic People's Republic of Korea (DPRK), Vietnam, India, and elsewhere.

Publicized readouts from the ILD's more recent student events show a shift from that earlier period. Instead of the department telling its own story, the ILD now answers Xi's call to "tell the China story well" (讲好中国故事). In early 2025, Vice Minister Lu told Johns Hopkins students that "the PRC has maintained a high degree of continuity in its policy towards the United States" (中国始终保持对美政策的高度连续性), and

rejected national responsibility for deteriorating U.S.–PRC relations (ILD, March 18, 2025). He also expressed hope that the students can "experience the genuine, three-dimensional, and multifaceted PRC" (感受真实、立体、全面的中国), a statement that contains common tropes related to "telling the China story" (ILD, March 18, 2025).

The content of meetings also reflects the ILD's shift away from purely managing the CCP's foreign relations. Conversations have expanded to cover general foreign policy topics, not just party-to-party ties. Lu's visitors from Harvard University asked questions concerning U.S.–PRC relations and cooperation, the PRC's policy in Latin America and the Middle East, and Russia's war in Ukraine (ILD, January 21, 2025). **[1]** Although presented as a technocratic tool to manage the CCP's relations with foreign political parties and advance broader foreign policy goals, this provides further evidence that the ILD has adapted to an era defined by perceptions of rising national power.

Table 1: Timeline of Public Meetings Between Foreign Students and ILD Leadership

Organizer	ILD Host	Date
University of Pennsylvania	Ma Hui	July 11, 2024
Columbia SIPA	Lu Kang	January 3, 2025
Harvard Kennedy School	Lu Kang	January 21, 2025
Johns Hopkins University	Lu Kang	March 18, 2025
China–U.S. Exchange Foundation (Beijing)	Lu Kang	January 6, 2026
Harvard University	Lu Kang	January 23, 2026

(Source: ILD, July 11, 2024, January 3, 2025, January 21, 2025, March 18, 2025, January 6, January 23)

Promoting PRC Global Leadership

In the past, changes to the ILD's mandate and value were motivated by external factors. The Sino-Soviet split that began in the late 1950s increased the ILD's significance by necessitating competition over relations with global Communist parties. Later, the dissolution of the Soviet Union and the end of the Cold War led the department to establish closer relations with non-Communist parties (Sutter, 2011). **[2]** These developments have translated into a growing scope for the department, which now deals with parties across the world and the political spectrum.

Unlike historical developments in the ILD's work, the introduction of student outreach in 2024 was the result of an internal shift: the PRC's growing comprehensive national power (CNP; 综合国力). By the 2010s, PRC policymakers and foreign policy experts determined that the country ranked second in terms of global CNP, motivating a more assertive foreign policy (China Brief, January 6). This confidence can be seen in then-minister Song Tao's (宋涛) comments on the department's role in 2016. He told a People's Daily reporter that since "the PRC finds itself at the center of the global stage for the first time" (中国前所未有地走近世界舞台中心), "one of the main characteristics of the Party's international work is political leadership" (政治引领是党的对外工作的主要特色之一). He elaborated, saying that the political exchanges the ILD are known for had become a means to achieve the goal of global leadership, rather than exchange being a goal in itself (People's Daily, December 28, 2016).

The shift toward promoting PRC global leadership in the 2010s has since guided the ILD's global engagement. In 2022, the department spent $40 million to build the Mwalimu Julius Nyerere Leadership School in Tanzania, investing in CCP-aligned education for members of African political parties (South China Morning Post, February 26, 2022). It has also worked with the CCP's traditional regional partners, such as the Cambodian People's Party, the Lao People's Revolutionary Party, and the United Russia Party to promote the One Belt, One Road (一带一路) initiative in their countries (Qiushi, August 16, 2019). These examples show the ILD promoting PRC global leadership

Table 2: Expansions of ILD Mandate Over Time

	1951–present	1990s–present	2010s–present	2024–present
Mission	Promote party-to-party ties		Promote PRC global leadership	
Outreach	Communist parties	All parties & "political rising stars"		Think tanks & universities

Note: Each period of expansion reflects additional responsibilities; the ILD continues to promote party-to-party ties and conducts outreach with Communist parties to this day. (Source: compiled by the author based on Robert Sutter's Historical Dictionary of Chinese Foreign Policy, Larry Diamond and Orville Schell's China's Influence and American Interests: Promoting Constructive Vigilance, and ILD materials)

Table 3: Recorded Think Tank Visits to ILD

Institution	Year
Brookings Institution	2025
Eurasia Group (2 visits)	
Carnegie Endowment for International Peace	
CSIS	
National Committee on U.S.–China Relations	
Asia Society Policy Institute	2024
Paulson Institute	
CSIS	2023
Asia Society Policy Institute	2019
CSIS	
National Committee on American Foreign Policy	
National Committee on American Foreign Policy	2018

(Source: Compiled by author)

abroad by drawing on the party ties that it has maintained for decades.

Over the last 15 years or so, the ILD also began hosting U.S. think tank delegations in Beijing. Since 2018, there have been at least 13 meetings with think tank representatives, ranging from research and policy organizations to U.S.–PRC exchange forums. These meetings were most frequent in 2025 (see Table 3). Think tank delegations represent the ILD's first move away from institutional actors and toward politically-adjacent, if not peripheral actors. Student visits represent a further consolidation of this pivot.

No longer defined by insecurity, the ILD has taken assertive steps, both in 2018 and 2024, to move beyond traditional relationships with political institutional actors. If the ILD's goal is to advance the PRC's international leadership, then their meetings with students suggest that they believe young Americans may be receptive to such aspirations. They also see the target students—all from policy programs at elite U.S. institutions—as potential future political leaders, and as such worthy of cultivating (or at least influencing) from as early a stage as possible. The ILD has long invited political "rising stars" to Beijing, and they likely now see elite American students as meeting this criterion (Hoover, 2019).

United Front Channels Mirror University Engagement

Most student delegations to the ILD have been organized by universities, but one visit in January 2026 was organized through CUSEF, which describes itself as promoting exchange and mutual understanding by "mobilizing all available resources" (动员一切可以利用的资源) (CUSEF (Beijing), accessed January 19). These resources have included its connections to PRC government entities and the CCP's United Front Work Department, a Party organ under the Central Committee dedicated to both domestic and international alignment with CCP interests.

CUSEF is supervised by the Chinese People's Association for Friendship with Foreign Countries (CPAFFC; 中国人民对外友好协会), a "mass organization" (人民团体) under the State Council (China Brief, June 21, 2024; CUSEF (Beijing), accessed January 19; Baidu Baike/中国人民对外友好协会, accessed February 10). CUSEF is also "guided" (指导) by a Hong Kong entity of the same name, which conducts similar work but places additional emphasis on high-level dialogues (CUSEF (Beijing), accessed January 19, CUSEF (Hong Kong), accessed February 10). CUSEF Hong Kong operates as a mechanism for foreign influence in the United States, with legal disclosures from 2010–2020 showing that it worked with seven lobbying firms to conduct outreach to House and Senate offices, and to manufacture think tank publications that align with Party narratives (China Brief, September 16, 2020). There is some overlap in the two organizations' governing personnel, including Elsie Leung (梁爱诗), the former first Secretary of Legal Affairs of the Hong Kong Special Administrative Region (China Brief, September 16, 2020; CUSEF (Hong Kong), accessed January 19). The Hong Kong entity's board of governors includes multiple representatives of the Chinese People's Political Consultative Conference (CPPCC; 中国人民政治协商会议), a central united front body that sits directly under the Party's Central Committee (CUSEF (Hong Kong), accessed January 19).

Conclusion

CUSEF's ties to the CCP explain why it would encourage American students to meet with the ILD, but the timing of the recent series of meetings shows how U.S. institutions have normalized these interactions. What might have seemed a step too far before 2024 now has an American-executed precedent. As the ILD brings

youth engagement into its scope of operations, U.S. universities and CUSEF alike provide a vector for the ILD to advance its goals of promoting Party interests and PRC global leadership.

Minister Song's comments on global leadership and the changing definition of "Enter the ILD" reflect the department's shift from a platform for exchange to one increasingly oriented toward promoting the PRC's global status. Foreign participants in ILD forums may not necessarily endorse PRC leadership or the Party's perspectives, but their participation likely reinforces the department's confidence, and provides it an additional layer of legitimacy. Given its expanded mandate since the 2010s, the ILD sees an opportunity to influence U.S. think tanks and universities, and meetings provide an outlet to assert its political aspirations as accomplished fact.

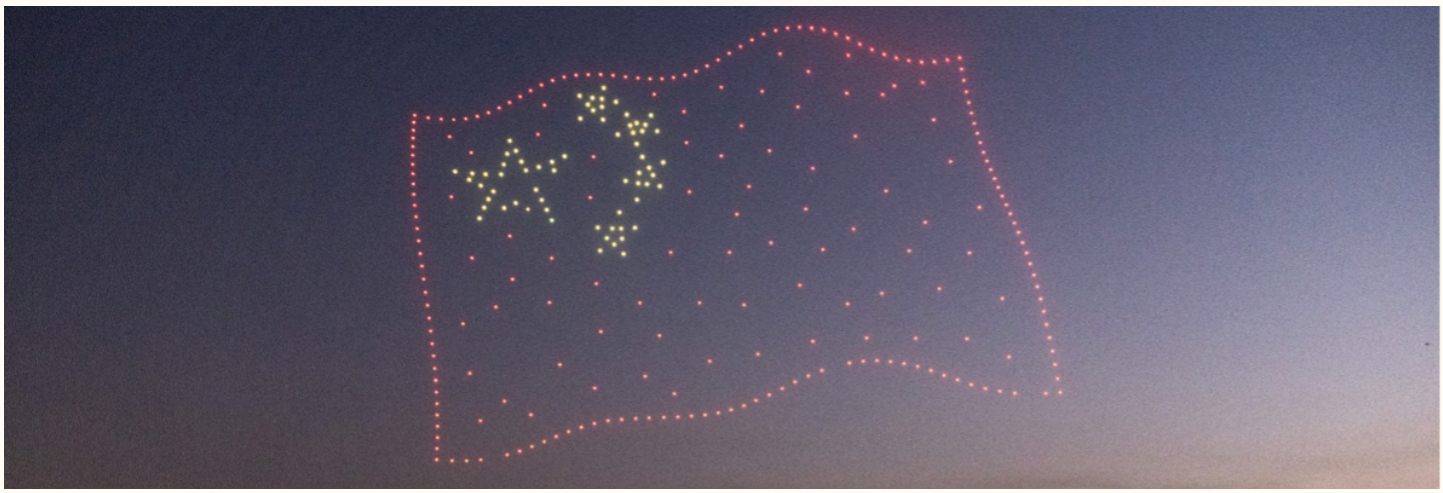
Jonah Reisboard is a research and editorial assistant at the Jamestown Foundation.

Notes

[1] Readouts from the University of Pennsylvania visit in 2024 and the CUSEF delegation in 2026 do not mention topics discussed. These readouts are limited only to a general outline of U.S.–PRC relations.

[2] Sutter, Robert G. Historical Dictionary of Chinese Foreign Policy. Bloomsbury Publishing, 2011, p. 128.

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



Drones form the Chinese national flag during Spring Festival celebrations at Expo Garden on January 25, 2023 in Wuhan. (Source: Getty)

The Low-Altitude Economy's Great Leap Upward

Youlun Nie
February 17, 2026

Executive Summary

- The People's Republic of China (PRC) has championed the low-altitude economy as a critical new engine for economic growth, yet the officially promoted market scale is significantly exaggerated.
- A severe lack of consumer-side demand renders the sector unsustainable. Its core applications are not economically competitive and long-term capabilities are constrained by technological bottlenecks and safety risks.
- Currently, the low-altitude economy relies on government investment, which is fiscally unsustainable. Even more dangerous is the exploitation of this concept by local governments for "asset fabrication," artificially manufacturing bubbles.
- The West often exhibits excessive alarm regarding the PRC's slogan-driven economic campaigns. Rather than a formidable competitive threat, the LAE represents a symptom of internal exhaustion—a speculative bubble engineered to absorb industrial overcapacity.

Amid a deepening real estate recession and diminishing returns on traditional infrastructure investment, Beijing has introduced a series of policy concepts aimed at stimulating growth. Among these, the "low-altitude economy" (低空经济) has emerged as a particularly prominent focal point.

Since the inclusion of the low-altitude economy in the 2024 Government Work Report as a representative "new quality productive force" (新质生产力), a campaign of state-directed industrial mobilization has unfolded nationwide (Xinhua, March 13, 2024). Official rhetoric envisions a market worth Renminbi (RMB) 2 trillion ($290 billion) by 2030, encompassing drone logistics, electric vertical takeoff and landing (eVTOL) aircraft, and massive airspace infrastructure (People's Daily, April 2, 2024). The initiative attempts to replicate the industrial policy success of the new energy vehicle (NEV), lithium battery, and solar photovoltaic sectors.

This goal is infeasible. Structural analyses of cost models and industrial chains show that low-altitude economy proliferation is currently driven almost exclusively by supply-side mandates rather than genuine demand-side traction. The sector lacks scalable commercial applications capable of forming a closed loop. Consequently, the actual market size likely remains orders of magnitude below official forecasts. The aggressive pursuit of this capital-intensive sector by local administrations, coupled with the current negative return on investment, risks exacerbating local fiscal crises, while the strategy of absorbing industrial overcapacity through technological substitution directly conflicts with a fragile employment structure in the People's Republic of China (PRC).

Government Framing Masks Reality

In the current PRC context, the low-altitude economy is a carefully reconstructed political-economic term. Transcending its traditional definition in general aviation, where it refers to civil aviation activity conducted in low-altitude airspace, PRC authorities now use the term to refer to a broader industrial ecosystem focused on manufacturing and infrastructure. But in policy guidance, Beijing is limiting the concept to refer to airspace below 3,000 meters, and often below 1,000 meters (Xinhua, September 27, 2024). This delineation circumvents the intractable issue of high-altitude military control, capitalizing on this "residual airspace" (存量空间).

The central government has escalated promotion of the low-altitude economy since it was first incorporated into the National Comprehensive Three-Dimensional Transportation Network Planning Outline (国家综合立体交通网规划纲要) in 2021. Momentum accelerated significantly following the Central Economic Work Conference in late 2023, which designated the sector a "strategic emerging industry" (战略性新兴产业). The subsequent implementation of the "Interim Regulations on the Flight Management of Unmanned Aircraft" (无人驾驶航空器飞行管理暂行条例) in 2024 provided standardized regulatory guidance for industrial development. Responding to these central directives, local governments have initiated "tournaments," launching a proliferation of projects that create the facade of prosperity (Xinhua, March 9, 2024, January 26).

Official forecasts also provide a deceptive image of profitability. According to the Civil Aviation Administration of China (CAAC) in late 2025, the PRC's low-altitude economy market size was expected to reach RMB 1.5 trillion ($220 billion) by the end of that year and RMB 3.5 trillion ($500 billion) by 2035 (Xinhua, December 23, 2025). These figures rely on a broad definition, however, that obscures a more prosaic reality. As outlined in the "Statistical Classification of

Low-Altitude Economy and Its Core Industries (Trial)" (低空经济及其核心产业统计分类(试行)), the term refers to a combination of four major categories of industry players: manufacturing, operations, infrastructure and information services, and support services (NDRC Low-Altitude Department, December 26, 2025). By aggregating all related sectors, official statistics blur the distinction between stock markets with relatively fixed demand—such as agricultural spraying and industrial inspection—and incremental markets in which new demand drivers are created. Stripping away legacy sectors, the burden of growth expectations falls on only two novel consumer-facing industries: drone logistics and eVTOL aircraft. But until organic consumer demand drives revenues in these areas, the purported market remains a mirage built upon fiscal subsidies and buttressed by state media hype.

Drone Logistics Are Not Economically Viable

Consumer adoption will serve as the litmus test for the low-altitude economy's viability. While established agricultural and industrial applications have matured, these specialized production tools are inherently limited by the finite scale of their downstream sectors. To bridge the gap between insufficient applications and economic strategy, official propaganda has touted urban last-mile delivery as the industry's primary breakthrough point (People's Daily, May 24, 2024). But this scenario faces severe economic and operational barriers.

A principal hurdle lies in unit economics. The PRC's logistics efficiency is predicated on the extreme utilization of the country's demographic dividend rather than on high technology. According to estimates based on financial data from Meituan, a delivery service, the average delivery cost for a human rider is approximately RMB 4.13 ($0.60) (Huxiu, March 25, 2025). This hyper-efficient ground network constitutes a cost barrier that drones cannot easily overtake. Conversely, the costs of drone delivery remain prohibitive. Meituan's operating data in Hong Kong reveals drone delivery fees as high as Hong Kong Dollars (HKD) 30 ($3.84), which executives admit fails to cover operational costs (The Standard, June 6, 2025). Even assuming economies of scale in the mainland, after factoring in equipment depreciation, ground battery-swap personnel, and pilot monitoring, the comprehensive cost per order remains significantly higher than that of human labor. In non-specialized scenarios, drone delivery possesses no comparative cost advantage.

Safety and political red lines in the PRC's highly centralized authoritarian system further constrain expansion. In urban areas, the potential risks extend beyond accidental crashes to encompass malicious attacks and espionage activities, involving unacceptable public safety and political liabilities. **[1]** In this context, Beijing remains extremely sensitive to airspace security. The capital's administrative region has been a strictly enforced no-fly zone and new national standards require civilian drones to install remote identification and countermeasure interfaces, effectively granting authorities a kill switch for commercial drones (Beijing Municipal Government, August 4, 2025; Xinhua, December 9, 2025). A business model that faces constant no-fly risks in core cities contains inherent limits to its national expansion.

Large-scale promotion of drone logistics may even present a gray rhino risk to social stability. The immediate delivery industry currently serves as a vital social stabilizer, absorbing over 13 million riders by 2024, most of whom are migrant laborers from rural regions (Huaon, December 15, 2025). However, technological substitution threatens to dismantle this employment reservoir, inevitably leading to mass structural unemployment.

eVTOL Aircraft Are Commercially Immature

If drone logistics is commercially unviable, the eVTOL sector resembles an industrial bubble designed to absorb excess capacity. Often dubbed "electric cars that can fly" (飞行汽车), eVTOLs share approximately 70 percent of their supply chain with NEVs, including batteries, motors, and carbon fiber composites (Securities Daily, March 7, 2025). For battery manufacturers and automakers grappling with "involution" (内卷) and overcapacity, promoting eVTOL development functions as a critical "spatial breakout" (空间突围) strategy. But this logic, based on supply-side spillover, encounters hard technological and safety constraints.

Current lithium battery energy density severely limits flight endurance. Industry insiders frankly admit that "very few brands can fly for more than 15 to 20 minutes," citing this as a "critical flaw." Even the most optimistic manufacturers concede that flight durations rarely exceed 30 minutes (BBC, May 16, 2025). After deducting energy consumption for vertical takeoff/landing and mandatory safety redundancy, the effective commercial range is negligible. Although some manufacturers have extended flight range by scaling up the airframe and battery capacity, this comes at a prohibitive cost, surpassing RMB 13 million ($1.8 million) per unit (Securities Times, February 11, 2025). At this price point, the industry is effectively reinventing the helicopter, but with significantly lower utility and higher capital costs.

Safety is the Achilles' heel for eVTOL aircraft. Unlike NEVs, an eVTOL power failure can result in a catastrophic fall. Market events since 2025 have undermined public confidence and led to the bankruptcy of German entity Lilium and the crash of a prototype from Xpeng AeroHT during a rehearsal (Yahoo Finance, February 21, 2025; BBC, September 17, 2025). For these reasons, the CAAC restricts flights to daytime flights in non-adverse weather conditions in which visual line of sight can be maintained. This compresses application scenarios and effectively reduces the technology to an expensive "aerial cable car" (Low Altitude Economy, March 25, 2025).

Commercially, eVTOLs face a small consumer base. For the public, ticket prices significantly exceed those of high-speed rail, rendering such transport largely unnecessary for daily needs (The Standard, February 2, 2025). Meanwhile, general aviation has historically struggled in the PRC, with small markets for private helicopters and aircraft. Even experts within the system acknowledge this. According to an expert at the State Information Center, a think tank under the National Development and Reform Commission (NDRC), high eVTOL production costs and low passenger capacity mean that early applications will "primarily serve a small, time-sensitive demographic willing to pay a premium, remaining far from large-scale societal adoption" (主要服务对时间敏感、愿意支付更高费用的小范围群体，距离全社会规模化推广普及相对遥远) (NDRC, December 30, 2024).

Government Investment is Unsustainable

In the absence of genuine consumer demand, the low-altitude economy depends heavily on government procurement and massive infrastructure investment to sustain the appearance of prosperity. Beijing is attempting to replicate the path dependence seen in high-speed rail and 5G by artificially creating application scenarios through enormous public spending.

Current orders in the low-altitude economy primarily come from local governments and their affiliated entities for applications such as patrols, mapping, flight performances, and emergency rescue. This model essentially represents an internal circulation of fiscal funds. With local finances under severe strain, relying

on continued state procurement of costly low-altitude services is financially unsustainable. Many so-called "mega-orders" are merely non-binding letters of intent or involve local government financing vehicles as buyers, primarily designed to generate market hype rather than address genuine operational or business needs.

Infrastructure construction displays similar shortsightedness. Local governments are rushing to build vertiports and 5G-A networks based on projected rather than actual demand. Unlike high-speed rail, which supports massive population mobility, low-altitude infrastructure lacks underlying commercial traffic. Initiatives such as the Xiong'an New Area's low-altitude economy demonstration zone—which encompasses multiple drone bases, testing facilities, and shared experimental sites—risks adding to local debt burdens without generating significant economic activity (Hebei Daily, April 22, 2025).

More alarmingly, government involvement has transformed the low-altitude economy itself into a tool for "asset fabrication." A prime example is Pingyin County's attempt to auction low-altitude franchise rights for RMB 924 million ($133 million) to a state-owned enterprise wholly owned by its own finance bureau (China Brief, February 3). Rather than fostering a genuine industry, some local governments are exploiting the low-altitude economy as a vehicle for financial engineering, leveraging administrative jurisdiction to mask systemic insolvency. Such state-led maneuvers only serve to further inflate this speculative bubble.

Conclusion

The PRC's vision for the low-altitude economy, under current economic and technical conditions, constitutes a strategic misjudgment. Decision-makers in Beijing are attempting to transplant the industrial logic that fueled prior successes to a sector that lacks fundamental consumer demand. Unlike NEVs, which displaced internal combustion vehicles through superior user experiences, the low-altitude economy offers a regression in terms of cost, convenience, and safety for mass-market applications.

Facing sluggish growth, the central government is heading down the path of supply-side mobilization, attempting to replicate economic miracles through administrative fiat. While the PRC possesses manufacturing advantages based on supply chain spillover, the conversion of capacity into economic benefit requires genuine demand. At present, this is negligible, and state-led demand represents debt that mortgages the future.

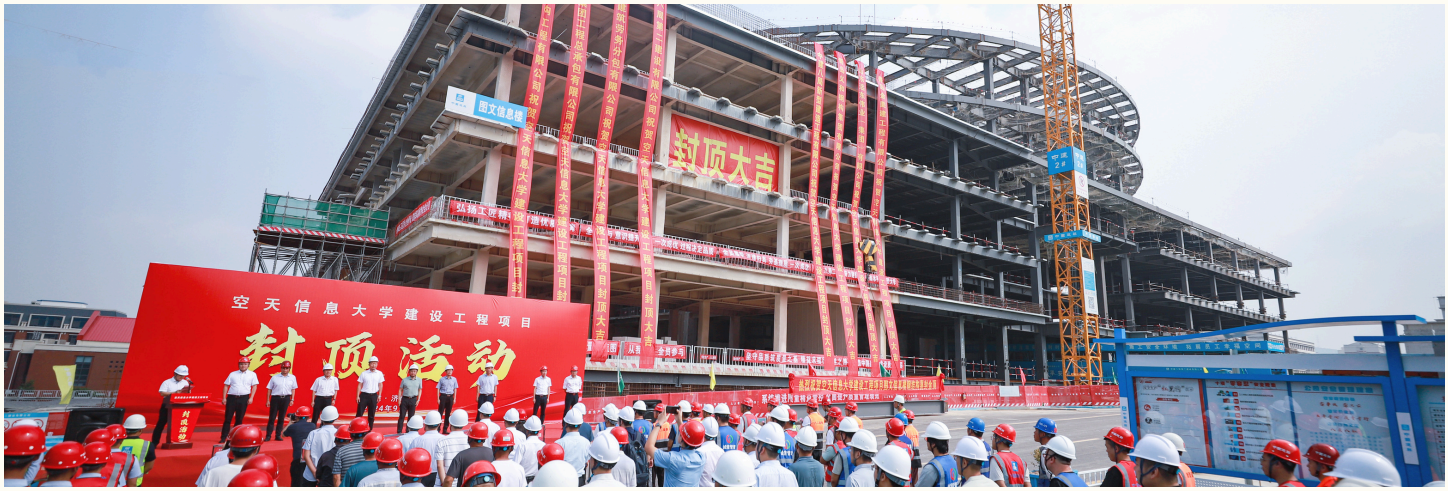
As fiscal subsidies recede, enterprises relying on speculative financing face bankruptcy, and infrastructure projects risk stagnation. This "new quality productive force" is poised to become another "unfinished project" (烂尾工程), stalling as it runs up against economic laws. Foreign observers should be less alarmed over competitive threats and more focused on the risks triggered by the inevitable burst of this bubble: the PRC's propaganda offensive might imply that the sky is the limit, but the reality is that the low-altitude economy is still struggling to get off the ground.

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] Such accidents have already taken place, as exemplified by a recent logistics drone crash in downtown Shenzhen (Lianhe Zaobao, February 10).

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



Aerospace Information University under construction in 2024. (Source: CSCEC)

PLA Reorganizes Space Information Support and Assurance Mission

Kristin Burke
February 18, 2026

Executive Summary

- The People's Liberation Army's (PLA) restructuring of its space information support and assurance forces further deepens its reliance on space for communications, navigation, and reconnaissance.
- The PLA is transitioning most—but not yet all—of the battlefield space information support and assurance mission to the Information Support Force (ISF) and the growing Chinese commercial space sector, freeing up the Aerospace Force (ASF) to build specialized capabilities and plans for offensive and defensive ground and space-based operations.

Executive Summary (continued)

- The Chinese Communist Party's (CCP) approval for a new civilian university to support communications, navigation, and reconnaissance ground-to-space integration not only helps smooth the handoff between the ASF and the ISF, but also demonstrates progress towards China's national plan for "air-space-ground integration."

The People's Liberation Army (PLA) is currently transitioning between "informatization" (信息化) and "intelligentization" (智能化) as part of its modernization agenda. As an important intermediate step—and following the 2024 reorganization of the Strategic Support Force into three separate arms (兵种) directly subordinate to the Central Military Commission (CMC)—it is transitioning the military space information support and assurance mission area from the Aerospace Force (ASF) to the Information Support Force (ISF). This will reduce organizational and technological "bottlenecks" (卡脖子) that impede timely fusion of multi-sensor information for joint warfighting. The transition is not yet complete, and it is unclear whether the PLA intends a full transition.

A new civilian university in Jinan, the Aerospace Information University (空天信息大学), is part of this overhaul. The institution aims to train ISF talent and the growing commercial space sector with the requisite capabilities to achieve PLA and broader Chinese Communist Party (CCP) goals in the 15th Five-Year Plan period (2026–2030). This will support deepening the "integration of communication, navigation, and remote sensing" (通导遥一体化) (Chinese Academy of Sciences [CAS], August 18, 2025; Xinhua; Jinan Daily, January 9).

PLA Reorganizes Space Operations

In recent years, the PLA has gradually adjusted the mission areas it includes under space operations. **[1]** According to a key 2024 text, Introduction to Space Operations (太空作战概论), space information support and assurance operations (太空信息支援保障作战) is now one of five such mission areas. **[2]** This newer mission is a combination of space information support, one of the oldest mission areas, and assurance, which previous PLA texts had described as needed but lacking. **[3]**

The CMC, the military's top decision-making organization, is currently transitioning units responsible for the space information support and assurance mission to the ISF, which oversees PLA network information systems and provides force-wide communications support, including secure strategic and tactical communications. This move is a logical one, as one of the CMC's goals for the ISF is to address the PRC's patchwork of information security and assurance efforts. The CMC also expects the ISF to lead integration and fusion of survey, mapping, remote sensing, meteorological, and positioning ground and space-based sensor data to provide battlefield intelligence support to PLA theater commands and services (U.S. Department of Defense, December 23, 2025). It is not transitioning all space information support units to the ISF, however, due to the PLA's division of units to support mission areas. For example, telemetry, tracking, and control (TT&C) for satellite and launch operations that underpin separate PLA mission areas will remain under the ASF.

The PLA has traditionally organized units under the space information support and assurance mission area into five or six functional groups. This has been done to create a division of labor for managing its space-based and ground-based infrastructure. **[4]** As of February 2026, most but not all of the space information support and assurance functional groups listed below have transitioned to the ISF. The groups are as follows:

1. **Space information acquisition units:** These collect battlefield information from reconnaissance, ocean surveillance, early warning and detection, meteorological, and mapping satellites.
2. **Positioning and navigation units:** These support reliable transmission of Beidou satellite information to ground, air, sea, and other military users' equipment.
3. **Space information transmission units:** These support the construction of space-to-ground communications links, integration, and fusion with space and ground reconnaissance intelligence, command and control systems, and various combat platforms, to include strategic and tactical satellite communication networks.
4. **Space information resource management units:** These ensure ground-based systems for receiving, processing, distributing, and providing access to information. They include service centers for managing marine environment remote sensing, meteorological data, and mapping, all of which catalog satellite information to provide users with standardized information for search and application.
5. **Ground application units:** These include two groups, an application support group and an end-user support group. The former manages the ground infrastructure that supports military applications of satellites; the latter converts the information into end-user applications, directly interfacing with commanders or weapon platforms.
6. **Space information security and protection units:** These units will eventually be composed of assigned, attached, or reinforced information security and assurance units, according to a 2014 PLA textbook. If needed, space information assurance will also be coordinated with other services and arms' space information defense capabilities.

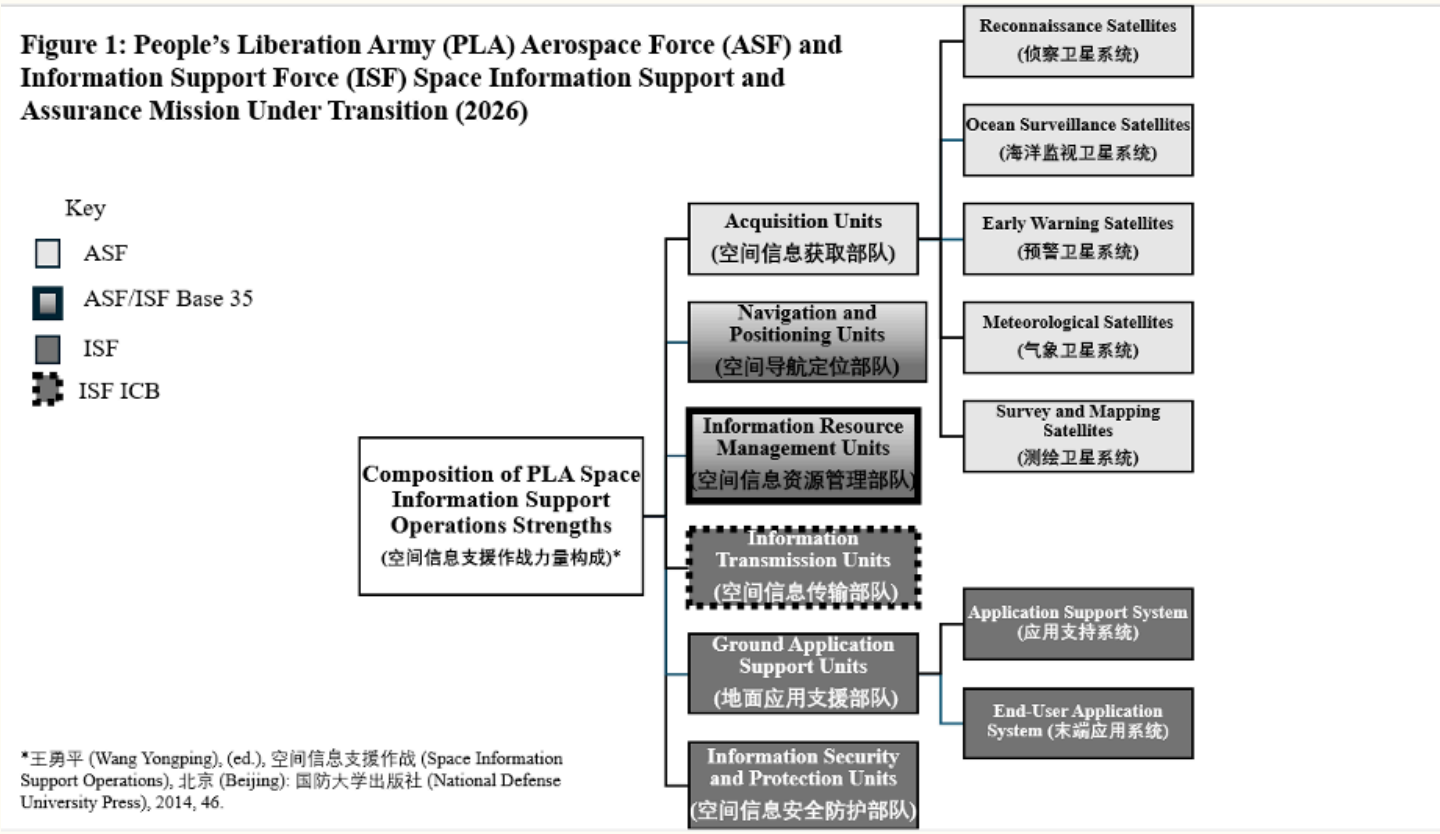
The CMC requires these functional groups to create workflows to support four space information support requirements for joint warfighting, according to the 2020edition of the PLA's Science of Military Strategy (战略学). These requirements are as follows: **[5]**

1. All-weather, near real-time space reconnaissance and surveillance, space surveying and mapping, and meteorological support capabilities to acquire and fuse information about enemy targets and combat environment, discover signs of war, monitor combat progress, evaluate combat effectiveness, and provide relevant information for force building, deployment, and use.
2. Secure satellite communication (SATCOM) capabilities to ensure the reliable, real-time, and confidential transmission of various intelligence information.
3. Satellite navigation, positioning, and timing capabilities globally for agencies, troops, weapon systems, and other spacecraft.
4. "Certain information integration and combat management capabilities."

Incremental Transition of Space Information Support and Assurance to the ISF

The PLA likely continues to organize its space information support and assurance mission area in this way, using the above six groups to support the four joint warfighting space information requirements (see Figure 1). The CMC has probably transitioned all spectrum and communications management to the ISF, including ground-to-ground connections and ground-to-space SATCOM links. But the ISF's control of space information support for other joint warfighting requirements is incomplete. Going forward, it may remain shared with the ASF and the growing civilian sector.

Figure 1: ASF and ISF Space Information Support and Assurance Missions Under Transition (2026)



Source: 王勇平 (Wang Yongping), (ed.), 空间信息支援作战 (Space Information Support Operations), 北京 (Beijing): 国防大学出版社 (National Defense University Press), 2014, 57-58.

The ISF is involved to varying degrees in all four of the PLA's joint warfighting requirements. Its role in supporting the first likely centers on managing the former Strategic Support Force's Base 35 (战略支援部队第三十五基地) and subordinate battlefield environment support brigades (战场环境保障大队) (China Brief, July 11, 2025; author research, 2026). Current Western understanding of the ISF and PLA military unit cover designators (MUCD) implies that the CMC would reorganize Base 35 under the ISF. But there are multiple indications that the transition is incomplete or that Base 35 will remain a joint ASF and ISF base in the near term. First, the ISF's new military unit cover designators (MUCDs) start at 32001; and the MUCD for Base 35 is 32020, which starts to abut what current Western researchers believe to be ASF MUCDs (CASI, December 11, 2023; China Brief, July 11, 2025). **[6]** As of February 2026, the author could not find clear designation of new Base 35 MUCDs as ISF units, which is inconsistent with the availability of information on the ISF more generally (author research, 2026). Second, while it is clear that the PLA's meteorological, survey, and mapping brigades fall under Base 35, the ASF and the ISF both continue to recruit applied meteorological technology experts (DXSBB, May 2025). Given that the ASF does not build meteorological satellites, they are likely recruiting meteorologists for launch centers.

The ISF's primary role in ensuring the second joint warfighting requirement is reflected in its management of the Information Communications Base (ICB) and subordinate

communications and spectrum brigades (Xinhua, June 30, 2011; China Brief, April 26, 2024; PLA Daily, May 19, 2024; Xinhua July 25, 2025). This was evident during the September 2025 military parade, which featured mobile SATCOM trucks within the ISF column. These trucks equip troops and theater commands with secure SATCOM links (CASI, September 15, 2025). The ICB primarily manages terrestrial communication infrastructure but also some ground-to-space links. It is too early to determine the fate of space-to-space links.

The ISF's role in ensuring the third requirement centers on positioning, navigation, and timing (PNT) applications. Remote sensing, mapping, and meteorology satellites all require PNT data from Beidou satellites to provide battlefield environment intelligence to commanders. But it is unclear if Base 35 currently manages the entire Beidou ground segment outside of receiving stations. This would include TT&C satellite control still under the ASF and time correction stations, which the PRC refers to as "injection stations" (China Argo Real-Time Data Center, October 8, 2018). These injection stations correlate all Beidou downlink data and then process and correct for normal timing errors before sending updates directly to satellites. Facilitating the Beidou inter-satellite data links and short message service that contribute to PLA missile reconnaissance and targeting will likely remain a joint effort.

For the fourth requirement, the ISF's role is probably a catch-all for the remaining and still evolving ways that spectrum management and space information support and assurance interface for joint warfighting. Potential indicators for this could include fusion between Beidou missile guidance and missile early warning satellite links, wider use of space-based space situational awareness in theater command planning, and adaptation to accelerating trends in remote sensing and communications satellites in Very Low Earth Orbit (VLEO). **[7]**

New Aerospace Information University

The restructuring of the PLA and national space information support and assurance mission area is ongoing. One piece of evidence for this is the approval in 2020 of a new civilian university in Jinan City, Shandong Province: Aerospace Information University. The project is a joint venture by Shandong Province and the Aerospace Information Research Institute of the Chinese Academy of Science (CAS). Since its approval, the university's construction was highlighted as a part of the province's 14th Five-Year Plan (2021–2025) and it has recruited its leadership team (Shandong Higher Education Circle, July 6, 2023; Baidu, July 23, 2025). But it is yet to properly begin operations.

Aerospace Information University will contribute to the PRC's national education ecosystem with a focus on "aerospace information networks, aerospace information materials and devices, earth observation, satellite navigation, and the Internet of Things" (空天信息网络、空天信息材料与器件、对地观测、卫星导航与物联网等领域) (Shandong Provincial Government, March 1, 2024). It is actively engaging with the PLA's Base 35, and other Wuhan City and Hubei Province-based universities, to support the base's geospatial and spatiotemporal workforce needs, both directly and through its collaboration with other Shandong-based universities (Shandong University, May 19, 2020; author research, 2026). Approval for the university does more than support PLA readiness and promote the economic efficiencies of dual-use technologies. It signals the progress that the PRC has made on what it calls "air–space–ground integration" (空天地一体化) over the last decade (Posts & Telecom Press, November 11, 2025). The 13th Five-Year Plan (2016–2020) envisioned connecting the

space, low-altitude, and ground economies with 5G, Beidou, and quantum security capability.

The new university is well positioned for its work on remote sensing technologies to contribute to this goal. Its leadership team includes Wu Yirong (吴一戎), the president of the CAS institute involved in the project. Wu recently led the development of the country's first VLEO synthetic aperture radar (SAR) satellite, Haishao-1 (海哨一号) (CAS, June 4, 2025). The world's first quantum microsatellite, Jinan-1 (济南一号), is also named for the city of Jinan. If successful, it could lead to enhanced security for the PLA's tactical and strategic communications, as well as national border and public security (Shandong TV News, August 1, 2022). The university is also one of a handful of projects supporting Shandong Province's Aerospace Industry Development Plan (山东省航空航天产业发展规划) for 2035. This plan focuses on creating applications for the integration of communications, navigation, and remote sensing data (通导遥一体化) (Shandong Provincial Government, March 1, 2024).

Conclusion

The organization of the PLA's information support and assurance units is an important signpost of PLA joint warfighting readiness and of the extent to which the ASF can deepen its expertise in other areas. Transitioning large portions of this mission to both the ISF and the growing commercial space sector frees bandwidth for the ASF to develop techniques, tactics, procedures, and operational plans for terrestrial and space-based operations. These are plans the ASF is obliged to make, given that the world has not yet experienced a war with tactical space-based confrontations and there are no historical lessons from which the PLA can draw.

The CCP's goals for the national space program extend well beyond the PLA's needs. Deepening civilian use and reliance on space systems beyond traditional PNT integration is aligned with CCP national innovation and economic development goals. These intertwining goals create research opportunities to understand the state of PLA readiness and Beijing's risk tolerance for instability in space.

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the Department of the Air Force, the Department of Defense, or any other U.S. government agency. Cleared for public release: distribution unlimited.

Kristin Burke is the Senior Space and Counterspace Researcher at the China Aerospace Studies Institute (CASI), under the U.S. Air Force's Air University. Prior to joining CASI she was a Deputy National Intelligence Officer for Space at the Office for the Director of National Intelligence and a China Science and Technology Analyst at the U.S. Department of State. She is proficient in Mandarin and studying aerospace engineering.

Notes

[1] Joel Wuthnow et al., eds., The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context (Washington, DC: National Defense University Press, 2021), https://ndupress.ndu.edu/Publications/Books/PLA-Beyond-Borders/.

[2] Jiang Lianju [姜连举], Taikong Zuozhan Gailun [太空作战概论] (Introduction to Space Operations) (Shanghai: Shanghai Shehui Kexueyuan Chubanshe, 2024), 136–144. Jiang is also the editor of Kongjian Zuozhan Xue Jiaocheng [空间作战学教程] (Lectures on the Science of Space Operations) (2013).

[3] Wang Yongping [王勇平], ed., Kongjian Xinxi

Zhiyuan Zuozhan [空间信息支援作战] (Space Information Support Operations) (Beijing: Guofang Daxue Chubanshe, 2014), 57–58.

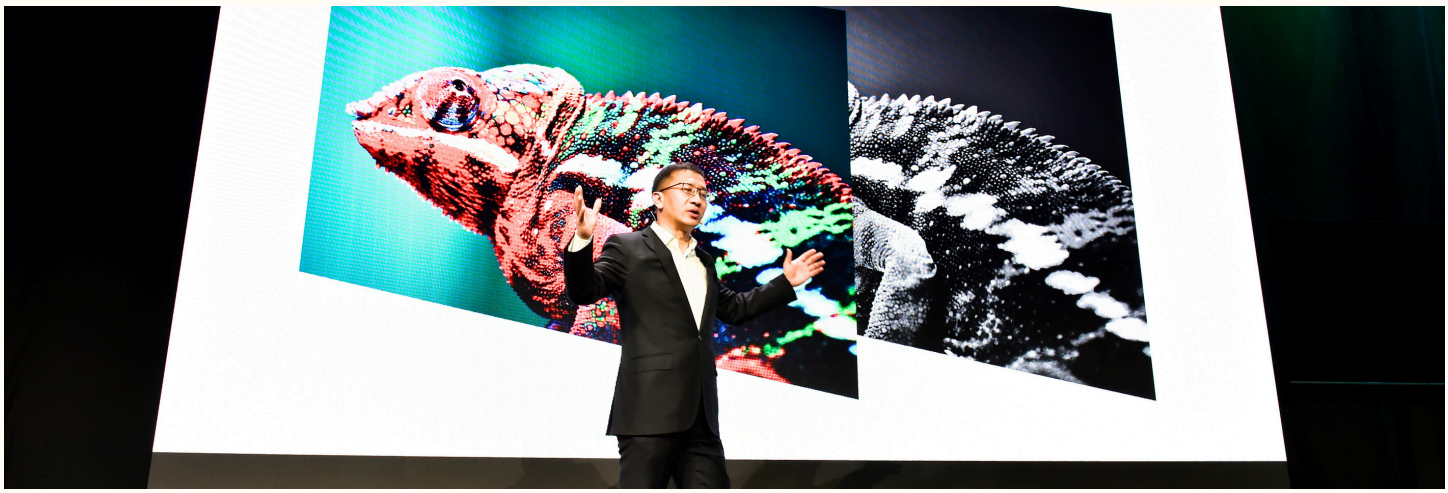
[4] Ibid.

[5] Xiao Tianliang, ed., The Science of Military Strategy, rev. ed. (Washington, DC: National Defense University Press, 2020), 397 (PDF 410), https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy.

[6] Kristin Burke, PLA Counterspace Command and Control (Maxwell Air Force Base, AL: USAF Air University, China Aerospace Studies Institute [CASI], 2023), https://www.airuniversity.af.edu/CASI/Display/Article/3612979/pla-counterspace-command-and-control/

[7] VLEO refers to altitudes below 400 kilometers.

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



International Vice President of Hisense Electronic Information Group Xiaohang Ma speaks during a press event for CES 2019. (Photo by David Becker/Getty Images)

Technical Analysis Reveals Connected Smart TV Security Risks

John Costello
February 20, 2026

Executive Summary

- Smart televisions manufactured by firms in the People's Republic of China (PRC) present national security risks across three categories: intelligence and surveillance, denial and disruption, and influence and manipulation. Risk profiles vary significantly by service model and manufacturer.
- The degree of original equipment manufacturer (OEM) control over the device stack ranges from total (proprietary platforms like Hisense's VIDAA) to partial but irreducible (platform partner models with Google, Amazon, or Roku), with the original design manufacturer (ODM) white-label model introducing an additional layer of supply chain opacity.

Executive Summary (continued)

- Data collection through automatic content recognition, OEM telemetry, and ecosystem linkages is extensive, and data residency claims are frequently contradicted or left ambiguous by the manufacturers' own privacy policies and technical infrastructure.
- The most consequential OEM capability is not data collection but the ability to modify device behavior at scale through over-the-air firmware updates, a privileged access point governed by engineering teams operating under PRC jurisdiction.
- PRC television manufacturers are expanding rapidly into adjacent smart home ecosystems, content services, and companion applications, transforming a discrete device risk into a persistent household-embedded data infrastructure whose complexity will grow increasingly difficult to govern.

At the technology trade show CES 2025, Chinese firm Hisense unveiled an "Urban Governance Platform" alongside its consumer electronics lineup. The platform, built by Hisense TransTech, a subsidiary founded in 1998, uses proprietary artificial intelligence (AI) chipsets and big data analytics to optimize traffic flow, streamline public transit, manage disaster prevention, and coordinate public safety operations. It is already deployed across 169 Chinese cities: in Qingdao, train schedules automatically adjust during rush hour based on crowd monitoring, traffic lights adapt based on pedestrian flow detection, and bus routes optimize in real time (Hisense USA, December 18, 2024; Yanko Design, December 19, 2024).

The same company whose AI-powered surveillance and governance technology is embedded in the infrastructure of numerous Chinese cities is also one of the world's largest television manufacturers. A state-owned enterprise operating under Qingdao's state-owned assets supervision and administration commission (SASAC), Hisense sells internet-connected smart televisions to tens of millions of American households. These devices run proprietary software, collect behavioral data, and receive firmware updates from engineering teams in Qingdao. Hisense is not unique. Television manufacturers in the People's Republic of China (PRC) have steadily extended their technical reach across the global TV market through acquisitions, licensing agreements, and original design manufacturer (ODM) relationships, often behind Western brand names.

The technical architecture of PRC-connected smart televisions may present risks to U.S. national security, even if these risks vary across manufacturers, service models, and device categories. The first three installments of this series built the case for examining these risks in layers. Part one documented the strategic policy cascade, from Premier Wen Jiabao's (温家宝) 2009 designation of the "Internet of Things" (IoT) as a "strategic emerging industry" (战略性新兴产业) through to the 2024 notice by the Ministry of Industry and Information Technology (MIIT) on "Intelligent Connection of Everything" (万物智联), which has driven PRC dominance in global IoT manufacturing (China Brief, July 25, 2025). Part two mapped the policy toolkit: state-owned telecom networks, protected domestic markets, standards diplomacy, and Digital Silk Road infrastructure bundling (China Brief, August 7, 2025). Part three descended to the organizational level: CCP party cells embedded in every major manufacturer, Data Security Law (数据安全法) obligations requiring cooperation with state security, and specific documented vulnerabilities in devices manufactured by the firms TCL and Skyworth (China Brief, September 19, 2025). This fourth installment turns to the technical substrate: the device architecture, service models, data flows, and

OEM capabilities that determine what these risks look like in practice.

A Framework for Connected Device Risk

Connected devices present three broad categories of national security risk. The first, intelligence and surveillance, involves the collection and exfiltration of data for espionage, behavioral profiling, or intelligence advantage. For smart TVs, this encompasses viewing habits captured through automatic content recognition (ACR), device fingerprints on local networks, voice recordings, app usage patterns, and household composition inferences derived from cross-device IP matching. The second, denial and disruption, involves degradation or manipulation of device function, ranging from individually bricking a device to coordinating firmware-level changes across large installed bases via over-the-air (OTA) update mechanisms. The third, influence and manipulation, involves shaping the information environment through content placement, factory-default app configurations, and preferential surfacing. This last category is less acute today, as content on smart TVs is largely dictated by third-party streaming apps. But it is growing more relevant as PRC manufacturers launch their own streaming services and content platforms.

These three risk categories do not operate in isolation. A device that collects household behavioral data (intelligence) could also serve as a vector for network disruption (denial) or as a platform for content manipulation (influence). And consequences cascade: a compromised smart TV affects not just the immediate user but the local network, linked smart home devices, and, at scale, potentially millions of households simultaneously. For consumer devices, these second order and aggregate consequences are where the real national security risk lies. But they are also the hardest to quantify.

Understanding where smart TVs fit in the broader landscape of connected devices is essential to assessing their risk profile. Connected devices exist on a spectrum. At one end sit commodity IoT products, such as thermostats, light bulbs, and basic sensors, with commoditized supply chains and minimal service-model complexity. At the other end are specialized systems like industrial control systems (ICS-SCADA) and telecom backbone equipment, with differentiated supply chains, known end-use environments, and consequence profiles that are visceral and quantifiable. Smart TVs occupy an uncomfortable middle ground. They have the service-model complexity of general-purpose computing devices, comprising multiple operating systems, app ecosystems, partner relationships, update pipelines, and advertising networks, but also the low-auditability and low-user-vigilance characteristics of commodity IoT. Consumers do not think of TVs as computers. They rarely check permissions, seldom update firmware manually, and do not run endpoint security software on them.

This distinction between scope-driven and scale-driven risk matters for policy. Specialized systems lend themselves to scope-driven assessment, which focuses on the consequences of a compromised device in a specific environment, evaluated against known operational contexts. The conventional ICTS risk assessment tooling, which includes entity lists, CFIUS review, and critical infrastructure frameworks, was designed for this mode. Consumer devices, by contrast, are scale-driven: supply chains are commoditized and opaque, there is no specific application context, and the primary drivers of consequences are market penetration, corporate and supply chain consolidation, and aggregate effect across all deployed devices. This is the analytical gap where smart TVs have been under-examined.

Technology

The analysis that follows applies two complementary lenses. The first is the adversary's perspective, which focuses on intent, access, and capability; in other words, what a state actor wants to do, what legal and structural access it possesses, and what the technical architecture enables. The second is the defender's perspective, which looks at threat, vulnerability, and consequence. Building on the preceding installments in this series, these are evaluated by examining devices' technical architecture and assessing additional risks that scaling brings via market penetration.

Smart TV Technical Architecture and Risk Surface

A smart television is built in layers. At the base sits the hardware and firmware layer: the system-on-chip (SoC), flash storage, network interfaces, and the boot chain that sequences from ROM boot through bootloader and trusted execution environment to the operating system kernel. Above that is the operating system itself: Google TV, Amazon Fire TV, Roku OS, or a proprietary Linux-based platform like Hisense's VIDAA or Skyworth's Coolita. The middleware layer sits between the operating system (OS) and the user-facing applications, and includes media codecs, digital rights management, hardware abstraction, voice assistant integration, and, critically, the device management and telemetry services where original equipment manufacturer (OEM) data collection lives. The top layer is the application environment: app stores, runtimes, sandboxing, and update channels. Each layer has a different owner, and the boundaries between them define the risk surface.

What matters for risk assessment is not the layers themselves but who controls each one and under what governance framework. That question is answered not by the device's brand or price point but by its service model. PRC-manufactured smart TVs generally follow one of three archetypes, each with a distinct risk profile.

- Proprietary OEM operating system: The manufacturer maintains control across every layer of the stack. Hisense's VIDAA platform is the clearest example. VIDAA is a Linux-based OS developed, maintained, and governed entirely by Hisense (Spyro-soft, May 22, 2025). The company controls the boot chain, kernel, middleware, application store, update pipeline, and data collection services. There is no external platform partner providing independent audit, sandboxing governance, or update oversight. If Hisense, a state-owned enterprise, is directed or pressured to modify device behavior, there are no structural firebreaks in the software stack to prevent it. VIDAA is now the second-largest smart TV operating system globally, powering approximately 30 million televisions across more than 180 countries (NextTV, June 10, 2025). In the United States, Hisense deploys VIDAA on select models while using Google TV or Roku on others, a dual-stack strategy that complicates per-device risk assessment but does not eliminate VIDAA exposure.
- Platform-partner model: This model introduces meaningful structural boundaries. When TCL ships a Google TV, Google controls the operating system, app store, and core middleware, while TCL retains control over the hardware, firmware, bootloader, and a vendor-specific partition within the Android software build that includes the OEM's telemetry, device management, and launcher customizations. Google's Play Protect and verified boot concepts provide some assurance at the OS and app layers, and TCL's vendor partition is approved during the certification process. But the extent of ongoing audit—what Google actually inspects in TCL's vendor partition, how frequently, and with what rigor—is deal-specific and not publicly documented. Roku TV and Fire TV impose similar but not identical boundaries,

- (continued) with Roku generally retaining much tighter platform-level control and Fire TV governance varying by OEM agreement. The platform partner model reduces the OEM's unilateral control over the software stack, but the firebreaks are partial: the OEM still controls the hardware and firmware layers beneath the platform, and its privileged middleware runs with elevated permissions on the device.
- ODM or "white-label" model: This model introduces a much different kind of product and branding opacity. Tongfang (同方), a Tsinghua University spin-off now 21 percent owned by China National Nuclear Corporation, the state-owned enterprise in charge of the country's civilian and military nuclear programs, manufactures televisions sold under the Westinghouse, Element, and formerly Seiki brand names (VentureBeat, January 3, 2017; MarketScreener, accessed February 20). When those devices run Amazon's Fire TV, the platform controls most of the software stack and consumer data flows terminate at Amazon, not Tongfang. But Tongfang designed the hardware, including SoC selection, board layout, network interfaces, and low-level firmware. that provenance is invisible to the consumer. A shopper buying an Element TV at Walmart has no indication that the device was designed and manufactured by a SASAC-affiliated Chinese state enterprise.

The common thread across all three archetypes is that the OEM—or, in the ODM case, the hardware integrator—retains some irreducible level of control. Even in the most constrained platform–partner arrangement, the manufacturer controls the physical device, the boot chain, and at least some privileged firmware. Given this fact, key questions for consideration must answer how deep such access runs, what governance measures constrain it, what is visible to partners and end-users, and what degree anyone outside the manufacturer is in a position to audit or verify claims.

Data Collection, Storage, and Access

Smart TVs collect data through three overlapping channels. The first and most scrutinized is automatic content recognition (ACR), a technology that captures what is displayed on screen and matches it against content databases to identify viewing behavior. TCL deploys ACR through a partnership with Samba TV, a privately held U.S. company whose technology is integrated at the chipset level across 24 smart TV brands and claims reach into 111 million American households (Samba TV, January 5, 2023, accessed February 19). Hisense deploys ACR through an exclusive global partnership with Nexxen (formerly Tremor International), renewed in August 2025 through at least 2029, which grants Nexxen direct access to viewing data collected through the VIDAA platform (GlobeNewsWire, October 26, 2021; Nexxen IR, August 11, 2025). Hisense's own Enhanced Viewing Service privacy notice names Nexxen as the ACR provider and describes how ACR-derived analytics can target advertisements on "other devices" sharing a household IP address (Hisense USA, March 1, 2025). Skyworth's former ACR partner, Gozen Data (勾正数据), a Beijing-based firm, went further: its software scanned local networks every ten minutes, collecting not just viewing data but device names, IP addresses, network interface identifiers, and the names of nearby WiFi networks—well beyond the television itself (The Register, May 4, 2021; EDN China, April 28, 2021). Skyworth terminated the partnership in May 2021 after public disclosure, but the incident illustrates how third-party data services embedded in smart TVs can operate well outside their stated scope. The second channel is OEM telemetry: device diagnostics, app usage, network environment data, and crash reports

Table 1: Per-Manufacturer Technical Summary

Manufacturer	OS Families	Service Model	OEM Control	Key Risk Factor
TCL	Google TV, Roku TV, Fire TV	Multi-platform portfolio	Medium–High (varies)	Largest global market share growth; multi-OS strategy means risk is segment-specific
Hisense	VIDAA (proprietary), Google TV	Dual-stack: proprietary + partner	High (VIDAA) / Medium (Android)	VIDAA gives full OEM control; #2 global smart TV OS
Skyworth	Coolita/Coocaa (domestic), Google TV (export)	Split by market	High (domestic) / Medium (export)	Explicit PRC access to data stored in India/Germany
TongFang	Fire TV, customer-specific	ODM integrator	Low (software) / High (hardware)	Brand opacity: consumer unaware of CNNC-affiliated manufacturer

Sources: Spyro-soft, 2025 (VIDAA architecture); NextTV, 2025 (VIDAA market share); MarketScreener, 2019 (TongFang/CNNC ownership); VentureBeat, January 3, 2017 (Fire TV Edition brands); Coolita Privacy Policy(Skyworth data access); Texas Attorney General, December 15, 2025.

collected by privileged, pre-installed applications that the user typically cannot remove. The third is ecosystem data. Hisense's privacy policy, for instance, explicitly describes using ACR-derived analytics to target advertisements on "other devices" sharing a household IP address, extending the television's data collection surface to phones, tablets, and laptops in the home.

Where that data resides—and who can access it—is much harder to pin down than it should be. Privacy policies and infrastructure evidence tell different stories depending on the company, the product line, and the vintage of the policy. Hisense's current U.S. Data Protection Policy states that its servers are "currently located in the United States of America," and DNS analysis confirms at least some infrastructure resolves to Amazon Web Services in Oregon (Hisense USA, April 30, 2023). But an older Hisense smart TV policy that is still within the lifecycle of devices in consumer homes explicitly permitted transfer of personal information to the PRC

(Hisense USA, January 1, 2020). TCL's global smart TV privacy notice reserves the right to "transfer, storage and process your information within and outside of your country," while its corporate privacy policy states that personal data "will be transferred and stored in Mainland China" (TCL Tech, October 15, 2024). Skyworth's Coolita OS policy is unusually transparent: cloud services are deployed in India and Germany, but "maintenance operations in China may access" data stored in those locations. This represents an explicit PRC access pathway regardless of where primary storage sits (Coolita, 2021).

The practical reality is that corporate domicile alone is an unreliable indicator of data residency. More actionable signals include named partners in privacy notices, service hostnames embedded in firmware and applications, and where those hostnames resolve, such as their cloud provider, geographic region, and network owner. This kind of infrastructure-level analysis reveals that even when a manufacturer claims U.S.-based hosting, the policy language often reserves broad cross-border transfer rights, and the specific location of consumer telemetry databases frequently goes unspecified. The gap between what privacy policies say and what the technical infrastructure does is itself a risk factor. And for PRC-connected manufacturers operating under article 35 of the Data Security Law (数据安全法) and article 7 of the National Intelligence Law (国家情报法), that gap takes on a different character than it would for a Western company with similar ambiguity. Deeper questions, such as the full scope of data collected, the infrastructure supporting its storage and processing, internal retention and sharing practices, and the identity of all downstream recipients, can ultimately only be answered by the companies themselves. This is where governments typically step in, whether through subpoena authority in the context of a national security investigation or a CFIUS transaction review. Absent a law requiring detailed disclosure of data collection, retention, use, and sale as a condition of participation in the U.S. market, the burden of discovery rests entirely on investigative authorities, an approach that is inherently reactive and limited to the cases that happen to attract scrutiny.

The Scale Problem

Smart televisions occupy an uncomfortable position in the national security landscape. They are not the specialized, scope-driven systems (like telecom backbone equipment, industrial control systems, or military platforms) that conventionally attract threat assessment and mitigation. High-profile devices in the most sensitive environments tend to receive the most attention, and for good reason: each compromised device in those contexts can produce outsized, cascading consequences, and the line separating tolerable risk from unacceptable exposure is comparatively clear. Defending critical infrastructure against supply chain compromise is a challenging but tractable problem—one that existing authorities like the Covered List published by the Federal Communications Commission (FCC), the Department of Defense's list of Chinese military companies (the CMC list), FASC, ICTS, and others are at least in part intended to address. Other, more outbound programs like the Commerce Department's Entity List can relieve some supply chain pressure in the long run, but do little to address dependence at home. Still, though, each of these programs only prohibit and constrain when a national security risk presents itself, at which point a commodity product has already achieved the market share and ecosystem diversity that makes its removal difficult and costly. There are few measures to shape these companies and their offerings as requirement of market participation.

Commodity consumer devices present the

Table 2: Data Residency Risk Summary

OEM	Privacy Policy Language	Infrastructure Evidence	PRC Access	Risk Level
Hisense	Current: "servers currently located in the United States." Older policy: permitted PRC transfer.	mytv.hisense.com → AWS ELB (us-west-2)	Documented in older policy	High
TCL	TV: "transfer… within and outside of your country." Corporate: "stored in Mainland China."	leiniao.com → Google Cloud; TCL Channel → AWS S3 (us-west-1)	Explicit in corporate policy	High
Skyworth	Cloud in India/Germany; "maintenance operations in China may access."	Coolita OS cloud services	Explicit operational access	Medium–High
TongFang	No consumer TV privacy policy found. ODM model: data flows to platform OS.	EU enforcement: employee data on PRC servers	Uncertain	Medium (opaque)

Sources: Hisense USA Data Protection Policy; Hisense Data Protection Policy (2020); TCL Tech Privacy Policy; TCL Global Privacy Notice; Coolita Privacy Policy; ViewDNS(DNS evidence); JDSupra(EU enforcement, TongFang).

inverse problem. The risk scope of any individual smart television is small. No single compromised TV in a suburban household is likely to produce a national security crisis. But smart TVs are not assessed individually—they are deployed at scale, across tens of millions of households, collecting behavioral data, receiving firmware updates, and integrating into expanding ecosystems of connected devices. The risk is measured in the aggregate: a composite net exposure where each device contributes a small quantum of intelligence value, surveillance access, or disruption potential that, summed across an installed base of this size, becomes unfathomably large. And the televisions themselves are only part of the picture. The companies that manufacture them are building outward, expanding into adjacent smart home ecosystems, content platforms, and companion applications, while simultaneously growing their market share through channels that attract little public scrutiny: OEM licensing

agreements, white-label partnerships, and ODM arrangements that embed PRC-engineered software stacks in devices sold under other brands. The scale grows, largely in silence.

At the core of this challenge is an uncomfortable asymmetry. Not every Chinese company is a national security threat, but any Chinese company could become one. This probability increases as a firm's market share, privileged access to user data, and potential usefulness as an intelligence asset grow. PRC law does not permit the kind of refusal or disclosure that would allow external observers to distinguish between a manufacturer that has been co-opted and one that has not—and no independent judiciary exists to check legal or operational overreach by state authorities. This is not a statement about intent; it is a structural observation about the legal and political environment in which these companies operate. Unfortunately, it is precisely the scale and market penetration that make these firms strategically significant that also makes a ban or "rip and replace" approach practically difficult or cost-prohibitive. The fifth and final installment in this series will examine the shifting risk dynamics of the smart television ecosystem—OEM capabilities, supply chain opacity, regulatory gaps, and the expansion trajectory that is transforming a bounded device-level risk into an open-ended one—and consider key challenges and considerations for governing it.

John Costello is a Non-resident Senior Fellow with the Carnegie Mellon Institute for Security and Technology, Director of Strategic Affairs at Wirescreen, and Principal with WestExec Advisors. He is the former Chief of Staff of the Office of the National Cyber Director, Deputy Assistant Secretary for Intelligence and Security at the Department of Commerce, and Deputy Executive Director of the Cyberspace Solarium Commission. He is an Adjunct Senior Fellow at the Center for a New American Security.

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

Defense minister Dong Jun at the 2025 Xiangshan Forum in Beijing. (Source: Beijing Daily)

Defense Minister Dong Jun Leading Contender for CMC Seat

Brandon Tran & Gerui Zhang
February 12, 2026

Executive Summary

- As Xi Jinping looks to rebuild the Central Military Commission (CMC), Defense Minister Dong Jun is a strong contender for elevation to the military's highest decision-making body.
- Dong's has operational experience as deputy commander of the Eastern Theater Command Navy, deputy commander of the Southern Theater Command, and commander of the PLA Navy, where he likely oversaw gray zone activities.
- Dong also has ties to Xi via the "Fujian Clique"—officers Xi worked with while a junior official in the southeastern province. Though the clique's most prominent members, He Weidong and Miao Hua, were purged from the CMC in October, Xi nevertheless appears to trust Dong, who remains the only three-star flag officer to reemerge intact after being placed under investigation.
- Xi selected Dong in 2014 to receive professional military training in Russia, another sign that Xi has previously seen him as both loyal and competent.

Executive Summary (continued)

- Beyond Dong, another contender is Major General Zhou Hongxu, head of the trusted Central Guards Bureau. One- and two-star flag officers may also be under consideration.

Chinese leader Xi Jinping has decimated the Central Military Commission (CMC). In 2012, the military's highest decision-making body comprised 10 individuals, in addition to Xi himself. Today, that figure is down to one. The most recent stage in Xi's purge, removing CMC vice chair Zhang Youxia (张又侠) and Joint Staff Department chief Liu Zhenli (刘振立), marks one of the most consequential rounds of elite military discipline in years (Ministry of National Defense, January 24). This development has significant ramifications on how the PLA will move forward with force modernization.

The most likely next step for Xi is to set about rebuilding the CMC, not least to remedy a sense of anxiety pervading the military that even he has implicitly acknowledged (People's Daily, February 6; China Military Online, February 11). In doing so, he will need officers with operational command experience in combat arms branches within their respective service. But he will require those officers to be sufficiently loyal (China Brief, February 11). This may lead him to turn to individuals he knew when he was a provincial official. He might also look to the PLA Air Force or Navy, as any PLA Army officers would likely be close to Zhang Youxia and Liu Zhenli, given the two generals' respective backgrounds. Another possibility is that Xi selects officers who have been sent to Russian command and general staff colleges for professional military education. Xi has already handpicked these officers once for their competence and loyalty; he might be inclined to do so again (LinkedIn/Dennis Wilder, February 1). Surveying senior PLA officers, only one individual meets all of the above criteria and therefore should be considered a strong contender for elevation to a new-look CMC. That individual is the current defense minister, Admiral Dong Jun (董军).

Defense Minister Top Candidate for New CMC

Dong Jun's professional résumé makes him a suitable candidate for the CMC. He was previously deputy commander of the Eastern Theater Command Navy, deputy commander of the Southern Theater Command, and commander of the PLA Navy (China Brief, February 2, 2024). His assignments with strategically vital theater commands handling the PRC's most salient national security interests make him a desired candidate for promotion by conventional force standards alone. Dong also has extensive experience overseeing gray zone activities, which are often conducted by the PLA Navy in the eastern and southern theater commands' areas of responsibility (Irregular Warfare Initiative, July 25, 2024). The ability to execute aggressive gray zone operations facilitates conventional force development by practicing applicable skills that can be transferred to kinetic combat scenarios (China Brief, March 25, 2022). If Dong were moved from his current, largely ceremonial role, his experience suggests he could help enhance PLA combat power generation.

Another reason why Xi might be willing to elevate Dong Jun to the CMC is that he seems to have a level of trust in his defense minister. Dong is the only three-star flag officer who appears to have reemerged with his position intact after being placed under investigation. [1] Dong's naval background also insulates him from Zhang Youxia's camp, which is composed of ground force, logistics/acquisitions, and rocket force personnel. He is also insulated by his ties to the "Fujian Clique" (福建系), a patronage network of officers whom Xi has personally cultivated since working with them while a

provincial official in Fujian (China Brief, March 15, 2025). This clique, however, was associated with He Weidong (何卫东) and Miao Hua (苗华), whom Xi purged from the CMC in October 2025.

The notion that Xi trusts Dong might therefore seem counterintuitive. It also contrasts with the analytic consensus when he was appointed to defense minister at the end of 2023. A common argument at the time was that Xi's decision not to include him as a member on the CMC or as a state councilor indicated a lack of trust (China Brief, January 17, 2025). But the decision not to promote Dong to the CMC earlier is not necessarily an indication of a lack of trust. It could reflect an intentional act to downgrade the office of the Minister of National Defense, perhaps out of a desire to signal that military diplomacy, especially with the United States, is a low priority (RAND, August 14, 2024; China Brief, October 4, 2024). In this reading, Dong Jun is not distrusted; rather, he simply has assumed a position whose duties have been limited to suit changing priorities.

Dong also meets the niche potential criterion of being an officer selected to attend professional military education courses in Russia. During his tenure as deputy chief of staff of the navy in 2014, Xi selected him to attend the Military Academy of the General Staff of the Armed Forces of the Russian Federation (China Times, February 8, 2024; Radio Free Asia, February 12, 2024). The analyst Dennis Wilder has argued that officers chosen to attend Russian command and general staff colleges exhibit clear leadership ability (LinkedIn/Dennis Wilder, February 1). No complete list of PLA officers selected for these professional military education opportunities exists in open sources, but Dong is the most senior officer known to have studied in Russia.

Beyond Dong Jun, Major General Zhou Hongxu (周洪许) stands out as another potential addition. Xi broke precedent in selecting Zhou to lead the Central Guards Bureau in 2021. Zhou also was reportedly responsible for the arrest of Zhang Youxia (LinkedIn/Dennis Wilder, February 1; China Brief, August 23, 2021). The bureau he leads is responsible for protecting the Party leadership and is therefore considered highly trusted (Sohu, January 7, 2025; Baidu Baike/中央警卫局, accessed February 12).

Xi could also elevate a younger generation of officers to the CMC. Purges have depleted the pool of three-star flag officers, requiring him to reach into the ranks of one- and two-star generals and admirals to backfill theater command, staff, and CMC positions.

Conclusion

The removal of all but one military member of the CMC leaves a hollow institution that Xi Jinping can shape as he desires. He may decide not to fill it to capacity at seven personnel (as he did in 2017 and 2022) or with exclusively military personnel. Dong Jun is the most likely candidate among the limited pool of remaining flag officers, though other possibilities include Zhou Hongxu and generals of lower grade and rank. Full confirmation will have to wait until the next plenary session of the Central Committee later this year. In the meantime, deeper study of the PLA's stock of senior officers should yield further insights into what the future of the Chinese military leadership might look like.

The views expressed are solely personal and do not necessarily represent the official policy or position of the United States Military Academy at West Point, the U.S. Army, the Department of Defense, or the U.S. government.

Brandon Tran is an International Affairs and Chinese double major at the United States Military Academy at West Point. He has interned with the Center for Naval Analyses, the Defense Intelligence

Agency, and the Army War College, working on Indo-Pacific security issues. He has been published in The Diplomat, Asia Policy, The Jamestown Foundation's China Brief, and more. Brandon was selected as a 2026 Rhodes Scholar and a 2025 Truman Scholar. Upon graduation in 2026, Brandon will commission as a military intelligence officer.

Gerui Zhang is an international affairs and Chinese double major at the United States Military Academy at West Point. He has interned with the Center for Naval Analyses and conducted independent research on discourse analysis in the People's Republic of China. His work on the People's Liberation Army has been published in The Jamestown Foundation's China Brief. Upon graduation, Gerui will commission as a logistics officer.

Notes

[1] In late 2024, Western media reported, based on U.S. government sources, that Dong was being investigated. This reporting was substantiated by Dong's absence from certain duties (China Maritime Studies Institute, November 29, 2024). PRC officials denied that this was the case, however, and Dong later resumed his role as minister of defense. This episode could indicate that Xi feels able to trust Dong.

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