中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

VOLUME 25 • ISSUE 3• FEBRUARY 14, 2025

IN THIS ISSUE:

Military Content Restrictions Could Indicate Trouble Ahead

By Arran Hope

Image from an instructional article about strengthening network security literacy among military personnel. (Source: Xinjiang Daily)

Executive Summary:

- New measures to control online information related to the People's Liberation Army (PLA) could be an indicator of imminent military operations, further purges, or other military activity.
- The measures are drafted by 10 military and state bodies, indicating that Beijing places enormous importance on information security and continues to pursue high-level military-civil integration.
- Possible motivations for the measures include recent leaks of sensitive information, online content that has reduced support for the military, and growing disinformation that has included spoofs of official websites. This compounds ongoing problems in the military, such as corruption.
- Beijing sees regime security and stability as downstream of controlling information flows, as well as dependent on building sophisticated regulatory and institutional capacity. The new measures support both these aims.

On February 8, the Cyberspace Administration of China (CAC; 国家互联网信息办公室) released a set of new measures to control online information related to the country's military, the People's Liberation Army (PLA). The "Measures for Managing the Dissemination of Military Information on the Internet (互联网军事信息传播管理办法)," which enter into force on March 1, will impose restrictions on the kind of information that is allowed to appear online, as well as on the entities that are allowed to publish it (CAC, February 8). **[1]**

A total of ten entities co-signed the measures, signaling the importance with which Beijing views them—an importance that is reflected in official commentaries published since their announcement. The two key organs involved are the CAC and the Political Work Department of the Central Military Commission (中央军事委员会政治工作部), and the cooperation between the two should be seen as evidence of military-civilian integration at the highest levels of the party-state. **[2]** Coordination between different entities on laws and regulations is common in the People's Republic of China (PRC), but the involvement of as many as 10 different military and state organs is less so. This suggests a substantial degree of concern about sensitive information appearing online.

Beijing Motivated by Need for Regime Security

The measures released last week were accompanied by a short transcript of a press conference about the regulations. These two items took up the entirety of page four of the following day's edition of the military's flagship newspaper, *PLA Daily* (PLA Daily, February 9, [1], [2]).

These documents all make clear that Beijing perceives the security of military information as critical for regime stability. As an official explainer declares at its outset, strengthening the management of military information "has a bearing on the overall situation of national defense and military construction, as well as on the image and reputation of the PLA (关系国防和军队建设大局，关系人民军队形象声誉)" (81.cn, February 9). In the words of another, network security and informatization "have a bearing on the long-term governance of the Party, and on the long-term stability of the country, its economic and social development, and the well-being of the people (事关党的长期执政，事关国家长治久安，事关经济社会发展和人民群众福祉)" (PLA WeChat, February 10).

There are internal and external factors that have led Beijing to this conclusion. Open-source information, including leaks and data on sensitive issues, can be accessed and used by the PRC's adversaries. Meanwhile, information about problems within the People's Liberation Army (PLA), such as high-level corruption or veterans' protests, could damage faith in the institution and loyalty to the regime (Kyodo News, August 2, 2024; China Brief, January 17). **[3]** The measures therefore should be seen in part as remedial efforts to mitigate these risks and shore up security for the regime.

One way in which regime stability is advanced is in the construction of "rule of law (依法治国)" society, a long-term goal of Xi Jinping. These measures support this ambition, contributing to a long list of regulations that have imposed more restrictions on and supervision of online discourse. As the measures themselves note, these include the 2017 *Cybersecurity Law*, the *Preservation of State Secrets Law* that was revised in 2024, the 2020 *Provisions on the Ecological Governance of Network Information Content*, and the 2022

Provisions on the Management of Information on Internet User Accounts. To this could be added an August 2024 proposal by the CAC in conjunction with the Ministry of Public Security (MPS; 公安部) for citizens to obtain cyberspace identification credentials, or the *Network Data Security Management Regulations* that entered into force on January 1 (Xinhua, August 24, 2024; People's Daily, October 10; China Brief Notes, October 24).

Related to this regulatory work is the development of executive and implementing institutions. The new measures seek to advance the regime's capacity in this area by encouraging more coordination between different institutions, including between military and state organs, furthering the military-civil integration that also has been a core part of Xi's agenda. As one explainer writes, the measures "require the military and local governments to work together and coordinate, and jointly manage [implementation] (需要军地协同联动、齐抓共管)." The third chapter of the measures, on "Supervision Management (监督管理)," begins by noting that the CMC's Political Work Department, the CAC, and other relevant departments at the central and local levels, have "established a coordinating mechanism (建立 … 协调机制)" for this purpose, and compels all of these organs to conduct activities such as daily inspections (日常检查) and random sampling (随机抽查), with the cooperation of service providers. The PRC's apparatus of digital repression is extensive, but even by those standards these new burdens appear to require an impressive level of coordination, effort, and resources.

The measures set out two approaches to content management. One is positive; namely, cultivating a favorable image of the regime and its core institutions. This comes through in the readout from the CAC press conference, which describes the measures' purpose and significance as "promoting the main theme and disseminating positive energy (弘扬主旋律、传播正能量)" (CAC, February 8). **[4]** The measures also evince a need for content to follow wider propaganda imperatives. Article 11, which appropriately lists 11 criteria for permissible military-related information, has as its first item content that "publicizes Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era and Xi Jinping Thought on Strengthening the Military (宣传习近平新时代中国特色社会主义思想，宣传习近平强军思想的)." The press conference transcript also states that following "Xi Jinping Thought on Strengthening the Military" should be the first guiding principle.

The second approach to managing content is negative—removing content deemed sensitive, harmful, or dangerous. Article 13 of the measures lists 12 kinds of content that are prohibited, beginning with that which "endangers national sovereignty, security, and territorial integrity (危害国家主权、安全和领土完整的)," but also including posts that "denigrate the absolute leadership of the Party over the army and the system of presidential responsibility of the CMC, and disseminate erroneous political views such as 'departyization and depoliticization of the army' and 'nationalization of the army' (诋毁党对军队绝对领导和军委主席负责制，散布'军队非党化、非政治化'和'军队国家化'等错误政治观点的)." Other parts of the measures also detail prohibited content. Article 10 forbids accounts that post military-related information from using names that include any of a large number of military-related terms (or those that employ homophonous or similar characters, symbols, numbers, or letters to approximate the same). Article 14, meanwhile, prohibits

content containing military secrets, national defense science and technology industry secrets, or unpublished information.

Measures Driven by Fear, Preempted by MSS & PLA Writings

Beijing's desire for measures such as these has been evident for several years. In 2021, an article in the magazine *Military Journalist* (军事记者) listed "four constant tasks (四个不断)" for managing the "online military environment (网络涉军生态)" and doing public opinion guidance work. The third item on the list, "on strengthening platform supervision and the control of communications," called for "accelerating the soundness of laws and regulations (加快法规健全)," including by formulating and improving rules on "the management of the dissemination of military information on the Internet (互联网军事信息传播管理办法)"—the exact wording of the title of the new measures (Military Journalist, May 2021).

In the months leading to their release, the perceived need for the measures became acute. In the civilian domain, the Party was rattled by a copycat article that impersonated its flagship newspaper the *People's Daily*, issuing a warning that such phenomena could "trigger a crisis of trust (引发信任危机)" (People's Daily, October 4). As the China Media Project observed, cases of alleged misuse of state media brands have been rampant in recent years, with the CAC documenting eight cases of netizens forging official government websites or documents to release false information in September alone (CMP, October 21, 2024). In the military domain, where information generally is more sensitive, Beijing sees untrustworthy content appearing online as even more serious. This has been a persistent problem, where there are many energetic military enthusiasts who historically have been a key source of information on PLA advancements. Several individuals have been arrested for photographing military bases and weapons, for example (Indian Express, February 10).

Fear underpins Beijing's desire for these measures, not just of disinformation but more critically of people leaking sensitive or classified information. Open-source intelligence (OSINT) and the advent of generative artificial intelligence capabilities have made it much easier to acquire publicly available information online and gain insights from it. In 2023, the U.S. government's Department of Defense stated its vision was to use OSINT as "the 'first resort' source of intelligence for decision makers and warfighters" (DIA, October 23, 2023). This has made Beijing vulnerable, as a December 2024 post on the official WeChat channel of the Ministry of State Security (MSS; 国家安全部) titled "Beware of Open-Source Information as a Source of Leaks (警惕开源信息成为泄密源头)" makes clear. "In the era of big data (大数据时代)," it begins, "the channels for putting out and disseminating information in cyberspace are becoming richer and more diverse (信息在网络空间发布、传播渠道愈发丰富多样)." It continues, warning that the Internet "has become an important source of open-source information for foreign espionage and intelligence agencies (成为境外间谍情报机关获取开源情报的重要来源)" who can use various methods to carry out "precise, continuous, and stable information tracking (对目标实施精准、持续、稳定的信息追踪)" to obtain valuable intelligence. Apparently, this is known to have taken place: the post admits that "occasional

breaches of confidentiality have occurred (失泄密问题时有发生)," in part unintentionally due to "videos taken by netizens (网友随手拍摄的视频)" (WeChat/MSS, December 1, 2024).

The MSS post proceeds to make the case for new measures. Although existing regulations require information to undergo confidentiality reviews before being made public, "it has been found that individual organs and units have failed to strictly fulfill the confidentiality review requirements when releasing information (但工作发现，个别机关单位在信息发布时，未严格履行保密审查规定)." As a result, the ministry recommends that relevant units should "strengthen the control of information disclosure from the source (加强信息公开管控)" and—crucially—that "platforms should strictly fulfill the main responsibility (网络平台应严格履行主体责任)" (WeChat/MSS, December 1, 2024).

This is exactly what the new measures call for: Article 6 states that Internet military information service providers (互联网军事信息服务提供者) must "set up … editorial organizations (设立 … 编辑机构)," while article 7 requires them to "conduct [account] verification (进行核验)" processes, article 8 compels them to make sure that military-related accounts and posts are appropriately designated as such, and article 9 requires that they keep a record of account holders' personal data. Article 7 also notes that editorial organs, content reviewers, and fact checkers must be "people with a high degree of political literacy, military professionalism, and confidentiality literacy (具备较高政治素养、军事专业素养和保密素养的人员)" (CAC, February 8).

The new measures inevitably will contribute to the continual hollowing out of PRC's digital domain. In 2019, China Brief lamented that information on the PLA already much more difficult than ten years prior (China Brief, July 31, 2019). This is part of a wider phenomenon. From July 2023 to July 2024, regulators removed over 57 million pieces of content and shuttered more than 4,800 websites and platforms (State Council, July 30, 2024). Chinese language websites as a proportion of all sites globally plunged by 70 percent in the last decade, in 2023 constituting just 1.3 percent of the total—a miniscule amount, considering that PRC citizens make up nearly one in five people on the planet (WeChat/He Jiayan, May 22, 2024; New York Times, June 4, 2024).

Conclusion

These measures, like most regulations, represent a reactive step taken by authorities. They follow apparent leaks of sensitive information, the publicizing of protests against the military establishment, and the proliferation of (at least some) copycat accounts spreading misinformation—all of which are damaging to the regime.

On another, potentially more dangerous level, they may also be proactive—or preemptive. Beijing has a history of shutting down online discourse, including on military topics, in advance of military or security operations. Recent examples include new censorship laws before activities in 2015 that militarized the South China Sea, controls on discussions about military movements and Taiwan policy before major military exercises around Taiwan in 2022, a crackdown on military bloggers before the 2020 India-China border clashes, and a ramping up of censorship of Hong Kong-related discussions prior to the violent suppression of

the protests that energized the city in 2019–2020. The question this raises is whether the new measures should be taken as an indicator of imminent military operations, further internal purges or reforms, or of other similar events to come. For now, this question is unanswerable, but it is one which will nevertheless remain central to future analysis.

Arran Hope is the editor of China Brief.

Notes

[1] Measures (办法) in the PRC context are a kind of implementation rule issued to clarify how a law or regulation should be executed. They have regulatory force but less authority than laws (法律) or administrative regulations (行政法规).

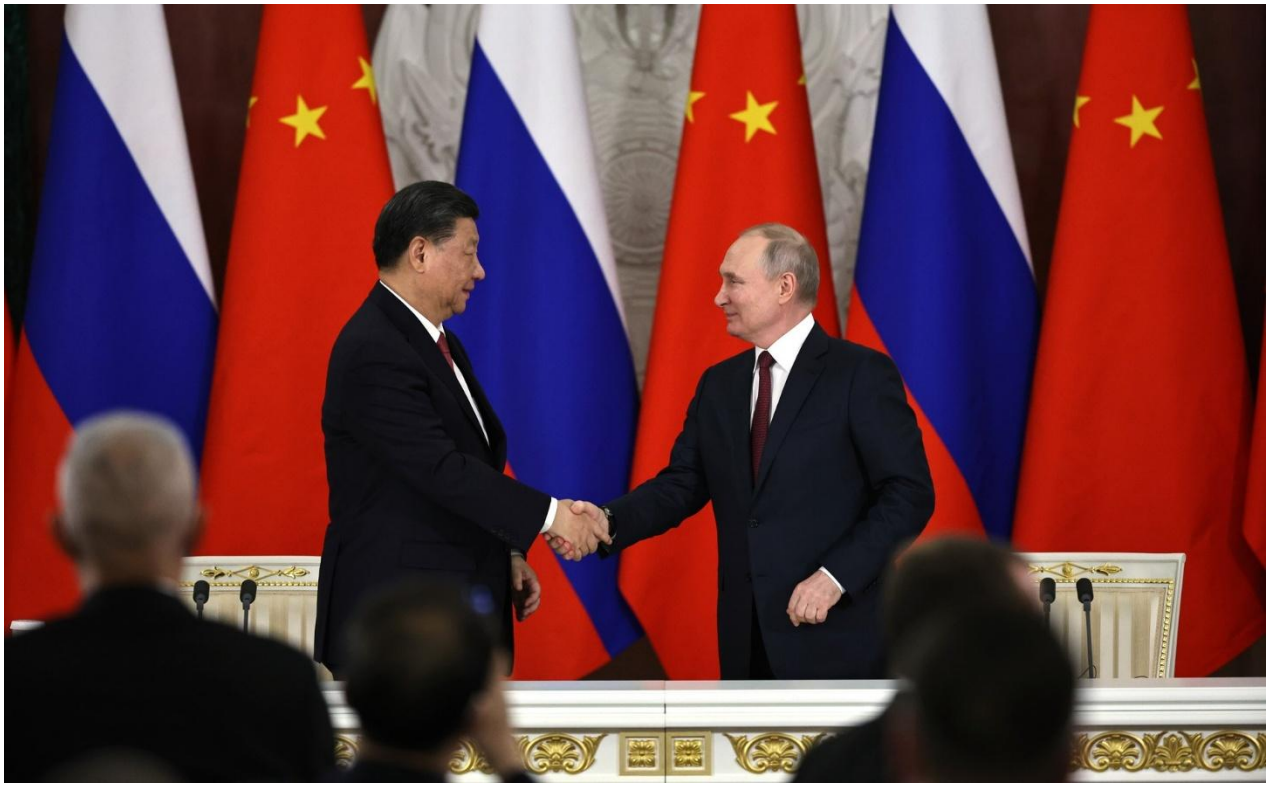
[2] The CMC Political Work Department oversees propaganda, morale, ideological indoctrination, and Party loyalty within the PLA.

[3] The measures themselves make oblique reference to this. Article 16 prohibits the dissemination of information that "incites military personnel, reservists, militia members, retired military personnel, and civilian personnel who have left the military to hold illegal assemblies, marches, demonstrations, and other activities that disrupt the social order (煽动军队人员、预备役人员、民兵、退役军人、退出军队文职人员非法集会、游行、示威等活动，扰乱社会秩序)."

[4] In CCP discourse, the "main theme" refers to the primary ideological line, and is always closely associated with "positive energy" in propaganda work (See Medium/David Bandurski, December 9, 2015).

Europe Could Be Supporting Russia's War via 'Seven Sons' Partnerships

By Ben Forney



Presidents Xi Jinping and Vladimir Putin meet in Moscow in 2023. (Source: Wikipedia)

Executive Summary:

- Research collaboration between European and Chinese universities could be indirectly supporting Russia's war against Ukraine.
- Over 20 agreements, partnerships, or newly published research articles have been announced between "Seven Sons of National Defense" universities and European entities between December 2024 and January 2025. These followed delegations from the universities to France, Austria, and Spain.
- The "Seven Sons" universities in the People's Republic of China (PRC) have a history of military collaboration, intellectual property theft, and, crucially, growing ties with Russia. They also have been implicated in talent recruitment programs that incentivize foreign experts to collaborate with PRC institutions, sometimes unknowingly contributing to military research.
- Unchecked research collaboration with the "Seven Sons" universities presents a real security threat. To date, the balance in Europe between scientific openness and national security tips toward the former. The longer the PRC continues to exploit this approach, the more that very openness will be put at risk.

In 2024, France and the People's Republic of China (PRC) commemorated 60 years of diplomatic relations. The two countries marked the occasion with both political fanfare and growing collaboration in science and technology research. PRC state media has framed these partnerships as evidence of the resilience of Sino-French ties, emphasizing ongoing and future joint ventures (CGTN, 2024; MFA, January 25, 2024; December 14, 2024). However, among these collaborations are exchanges with the "Seven Sons of National Defense" (国防七子)—a group of universities affiliated with the Ministry of Industry and Information Technology (MIIT; 工业和信息化部) known for their deep integration with the People's Liberation Army (PLA) and the country's military–industrial complex (ASPI, November 25, 2019; China Brief, June 7, 2024). **[1]** These seven universities are on the U.S. government's entity list, which details foreign individuals, companies, and organizations deemed national security concerns (eCFR, accessed February 10). **[2]**

PRC state media often present collaborations in the familiar language of "win-win cooperation" (合作共赢), portraying them as benign academic exchanges. For instance, a recent article in the *People's Daily*, the flagship newspaper of the Chinese Communist Party (CCP), featured a French robotics professor at Nanjing University of Science and Technology promoting Franco-Chinese technological cooperation (Xinhua Net, August 21, 2024; *People's Daily*, January 8). However, beneath this narrative lies a significant security risk for European institutions. "Seven Sons" universities have a history of military collaboration, intellectual property theft, and, crucially, growing ties with Russia, as exemplified by President Vladimir Putin's visit to the Harbin Institute of Technology (HIT; 哈尔滨工业大学) last May (HIT, May 18, 2024).

One implication often overlooked by European governments, universities, and even private technology firms engaged in partnerships with Chinese institutions is that many of these same Chinese universities are simultaneously working with Russian entities on dual-use technologies (Acta Astronautica, accessed February 10). As such, European research partnerships could be indirectly supporting Russia's war in Ukraine and harming Europe's own security as a result.

'Seven Sons' Research Enhances PLA Capabilities

The PRC's military-linked universities are actively engaged in research on a wide range of dual-use technologies. A focus on critical areas such as artificial intelligence (AI) and nanotechnology, which are poised to shape power projection capabilities in the coming years, is expected for such institutions. The "Seven Sons'" partnerships overseas provide concrete evidence of how they pursue these technologies. The collaborations outlined below align closely with key technologies targeted by the PLA as identified by the U.S. Department of Defense's (DoD) December 2024 report, *Military and Security Developments Involving the People's Republic of China.* These include AI; quantum information; brain science; biotechnology; clinical medicine; deep space, deep sea, and deep earth technology; and integrated circuits. The report also notes that the PRC is invested in photonics, nanoelectronics, network communications, robotics, and new energy systems (DoD, December 2024, p. 24).

Through the country's military-civil fusion (军民融合) development strategy, Seven Sons universities are deeply involved in supporting military modernization within the PRC. Historically, the PRC has leveraged international academic exchanges to gain access to critical technologies that support PLA modernization

efforts (U.S. Senate, 2019). Investigations have linked these institutions to economic espionage targeting Western research institutions and companies (Justia, accessed February 10). The blurred lines between civilian and military research in the PRC mean that academic breakthroughs can directly enhance PLA capabilities. It is for this reason that, in 2020, the Trump administration issued Proclamation 10043, which prohibited PRC students affiliated with the "Seven Sons" and other military-linked universities from obtaining visas to study in the United States (Federal Register, accessed February 10).

The universities also have been implicated in talent recruitment programs, such as the Thousand Talents Plan (千人计划), which incentivizes foreign experts to collaborate with PRC institutions, sometimes unknowingly contributing to military research (ASPI, August 20, 2020; China Brief, June 6, 2024). Other organizations, such as the Chinese Scholarship Council (国家留学基金委员会), recruits overseas students and scholars affiliated with weapons science and aeronautics to return to the PRC to continue their research (China Brief, October 8, 2019; DoD, December 2024, p.29, p.155). The "Seven Sons'" deepening ties with European institutions therefore raise concerns regarding the security of intellectual property and the military applications of their research.

Europeans' exposure to the kinds of risks these partnerships entail is not unique. American institutions are also deeply enmeshed in research collaborations with "Seven Sons" universities, as are other developed democracies such as Australia and South Korea (U.S. Senate, January 30; Data Abyss, accessed February 10). European institutions pride themselves on maintaining open academic exchange and fostering innovation independent of geopolitics. However, the risks posed by deepening ties with Chinese defense-linked universities remain poorly understood, with some prominent voices in academia even calling for closer ties with the PRC (The Times, December 25, 2024). Analyzing these latest partnerships provides insight into the research priorities of these universities for the coming year. Given their close ties to the Chinese military and government, the collaborations also offer an indirect glimpse into the strategic focus of these state entities. Additionally, the partnerships reveal that the PRC targets not only European universities, but also technology companies and international agencies. Yet European entities continue to expand these partnerships, despite the security risks they entail.

European Universities' Strengthening Ties to 'Seven Sons' Universities

In the past two months, institutions across Europe—not just in France—have established or strengthened links with at least one of the "Seven Sons." According to press releases from PRC universities, over 20 agreements, partnerships, or newly published research articles have been announced between these institutions and European (including Russian) entities between December 2024 and January 2025 (see below). While European policymakers focus on expanding export controls and countering Beijing's influence operations, the issue of research collaboration with PLA-linked universities has received comparatively little attention (BBC, December 17, 2024; Reuters, January 16).

Recent academic exchanges highlight the scope of the PRC's influence efforts. For example, in the week of December 9–16, 2024, Beihang University's president led a delegation to France and Austria that secured new agreements with leading institutions based in those countries. The delegation met with representatives from the International Atomic Energy Agency, the United Nations Office for Outer Space Affairs, and even

Nobel Laureate in Physics Albert Fert. Organized under the Beihang-Europe Cooperation Committee (北航中欧合作委员会), founded in 2023, these meetings culminated in new cooperation agreements in high-tech strategic sectors with both civilian and military applications. Among the key engagements were (Beihang University, December 16, 2024):

- A meeting with Olivier Chansou, president of the École Nationale de l'Aviation Civile (ENAC), focusing on expanding the Zhongfa Aviation Institute of Beihang University (北京航空航天大学) (ENAC, accessed February 10; Zfai, accessed February 10). According to a Beihang press release, the engineering school, which actively recruits international students and faculty, has been designated an "Excellent Case of Sino-Foreign Cooperation in Education" (中外合作办学优秀案例) in Zhejiang Province (Beihang University, December 25, 2024). Given the PRC's ambitions in aerospace, particularly through the state-backed Commercial Aircraft Corporation of China (COMAC, 中国商飞), and longstanding concerns over intellectual property theft related to the company's C919 single-aisle aircraft, such collaborations merit closer scrutiny from the French government and France's airline powerhouse Airbus (China Brief, May 10, 2024; USTR, May 14, 2024, p.34; Euronews, January 3).
- A renewed memorandum of cooperation with Austria's International Institute for Applied Systems Analysis (IIASA), emphasizing AI, big data, and complex systems research (IIASA, accessed February 10).
- A strategic cooperation agreement with Dassault Systèmes, a leading software firm, to develop a digital research and education platform, with planned joint research in AI, the metaverse, integrated circuits, and more (3DS, accessed February 10).
- A memorandum of understanding with leading engineering and research institution ESPCI Paris, facilitating joint research in chemistry, energy, and materials science (ESPCI, accessed February 10).
- A scholarship agreement with French mathematics foundation Fondation Mathématique Jacques Hadamard to support Beihang undergraduates pursuing master's degrees in France (Fondation Hadamard, accessed February 10).
- A collaboration with engineering institute INSA Toulouse focusing on joint research projects and meetings (INSA Toulouse, accessed February 10).

Beihang's December engagements extended beyond France and Austria. That same month, a delegation from its School of Integrated Circuits visited Spain's Catalonia Institute of Nanoscience and Nanotechnology at the Autonomous University of Barcelona to discuss joint research on two-dimensional materials, which are critical to military applications in sensors, imaging, and electronics (Beihang University, December 12, 2024; Defense Science Journal, accessed February 10). Meanwhile, a representative of Northwest Polytechnical University (NPU), Party Committee Executive Vice-Secretary Cheng Jiwei (程基伟), also met with the Autonomous University of Barcelona as well as with other Spanish universities as part of the China-Europe University Presidents Dialogue (中欧大学校长对话会) (NPU, December 9, 2024). As part of the trip, NPU

signed an agreement with the University of Salamanca to collaborate on aeronautical engineering and environmental science projects (University of Salamanca, December 12, 2024).

In addition to formal partnerships like these, there are numerous announcements of visiting lecturers and honorary scholars—many likely recruited through the PRC's talent programs—along with joint research publications and participation in international events (China Brief, August 5, 2010; NUAA, November 30, 2024; BIT, December 6, 2024; HIT, December 30, 2024; HEU, January 27). Collaborations span a wide range of fields from materials science to AI to energy. **[3]** Many of these areas of foundational research have direct applications that could contribute to military technologies, giving researchers from "Seven Sons" institutions early access to critical breakthroughs.

Europe's Indirect Support for Russia's War

In parallel with collaborations in Western Europe, PRC universities are strengthening their research ties with Russian institutions (Eurasia Daily Monitor, March 4, 2024). In late 2024, Andrey B. Prokofev, vice president of Russia's Samara University and faculty member of the Department of Aircraft Engine Theory, met with the leadership of both Nanjing University of Aeronautics and Astronautics (NUAA) and NPU (Samara University, accessed February 10). At NUAA, both sides reaffirmed their commitment to advancing international research collaboration, signing agreements to establish joint laboratories and dual-degree programs (NUAA, November 28, 2024). At NPU, Prokofev discussed talent cultivation and scientific research, culminating in an agreement to create a Sino-Russian joint research laboratory (NPU, December 2, 2024). Around the same time, Mikhail Gordin, president of Bauman Moscow State Technical University, visited Beijing Institute of Technology (BIT). The two delegations discussed strengthening cooperation in areas such as underwater robotics, lunar rover development, satellite platforms, and solar panels. They pledged to establish joint laboratories and enhance student and faculty exchanges (BIT, December 24, 2024).

The "Seven Sons" universities' collaboration with Russian institutions adds another layer of complexity to European engagement with the PRC. As Russia's full-scale war on Ukraine enters its fourth year, the strengthening of Sino-Russian research ties suggests the possibility of indirect European contributions to Russian military capabilities. Sino-Russian cooperation extends to critical sectors such as aircraft engines and aerospace propulsion—fields with direct military applications, as demonstrated by partnerships between Samara University and NUAA or NPU. Given the heavy sanctions Western governments have imposed on Russia's defense sector, PRC assistance to help sustain Russia's technological development could undermine European objectives.

Conclusion

European policymakers and academic institutions exhibit a persistent lack of urgency regarding the implications of such collaborations. Unlike the United States, which has taken some proactive measures to restrict academic exchanges with PLA-affiliated institutions, Europe's approach remains largely permissive (House CCP Select Committee, May 9, 2024). Emphasis on open research and innovation and the assumption that scientific progress exists in a geopolitical vacuum exposes it to strategic vulnerabilities. This is increasingly untenable in a world where technology is a cornerstone of great power competition.

Unchecked research collaboration with the "Seven Sons" universities presents a real security threat. To date, the balance in Europe between scientific openness and national security tips toward the former. The longer PRC continues to exploit this approach, the more that very openness will be put at risk.

Ben Forney is an East Asia security and risk consultant, based in South Korea. He holds a PhD from Seoul National University and is the author of The Spy Hunter newsletter on Substack.

Notes

[1] The universities of the Seven Sons of National Defence include:

- Beihang University in Haidian, Beijing
- Beijing Institute of Technology (BIT) in Haidian, Beijing
- Harbin Engineering University (HEU) in Harbin, Heilongjiang
- Harbin Institute of Technology (HIT) in Harbin, Heilongjiang
- Nanjing University of Aeronautics and Astronautics (NUAA) in Nanjing, Jiangsu
- Nanjing University of Science and Technology (NUST) in Nanjing, Jiangsu
- Northwestern Polytechnical University (NPU) in Xi'an, Shaanxi

[2] Academic research collaboration between "Seven Sons" universities and Western institutions is a widespread problem. According to recent testimony delivered by Dr. Jeffrey Stoff to the U.S. government Senate Foreign Relations Committee, "There were 17,630 unique articles published between 2019 and January 2025 involving a coauthor from one of these 'seven sons' defense universities and a coauthor affiliated with a U.S. institution" (U.S. Senate, January 30, p.11). Stoff highlights one case in which a former UCLA professor, who worked on DoD and NSF-funded research, "partnered with and had talent program appointments at the Beijing Institute of Technology (BIT) and other PRC research institutions heavily involved in defense R&D." He notes that no action was taken, and that the professor "now leads a massive AI research effort" in the PRC (p.27).

[3] A fuller—though non-exhaustive—list also includes chemistry, nanotechnology, carbon neutrality, big data, complex systems, the metaverse, simulation, digital healthcare, integrated circuits, and two-dimensional materials.

Five Key Factors Behind Irregular Leadership Changes in the People's Liberation Army

Zi Yang

The CMC Attends Spring Festival Gala Honoring Retired Officers, January 29, 2024. (Source: PLA Pictorial)

Executive Summary:

- The year 2024 witnessed sudden removals of high-level People's Liberation Army (PLA) commanders, a continuation of the purge of 15 defense industry leaders and military commanders in 2023.
- Xi Jinping's possible motivations include combating corruption, managing factional conflicts, asserting dominance as an aging autocrat, overcoming limited military service experience, and following successful historical precedents for control.
- The leadership disruption is expected to result in loyalty-based appointments, impair the PLA's combat effectiveness, and generate insecurity among officers, weakening morale and operational readiness.

Xi Jinping, Chairman of the Central Military Commission (CMC), continues to purge top commanders in the People's Liberation Army (PLA). In 2024, this purge targeted those at the pinnacle of the PLA—current and former CMC members who worked with Xi on a regular basis (PLA Daily, January 8). **[1]** This constitutes a step up from 2023, when Xi's anti-corruption campaign led to the downfall of 15 defense industry leaders and military commanders from the Rocket Force, Navy, Air Force, and CMC Equipment Development Department. The upheaval from the dismissals is expected to impair the PLA's effectiveness as a military force.

Five Perspectives for Understanding the Purge

Five possible explanations lie behind the purge of top PLA commanders: a genuine desire to eradicate corruption from the PLA, a need to resolve factional conflicts, Xi's paranoid psychology as an aging autocrat, insecurities stemming from the "peace disease," **[2]** and the success of previous purges. The first is the most common explanation for the abrupt removal of PLA leaders. Both corruption and factional infighting are endemic to the military. As is typical of autocrats, Xi is paranoid about threats to his power, which not only heightens fears for his own position but also concerns about the PLA's capabilities to deal with perceived mounting threats, which informs the third and fourth reasons. Finally, past precedents give him the confidence to execute his policies and remove high-level officers (China Brief, December 10, 2019).

The Anti-Corruption Angle

Corruption in the Chinese military is a decades-old problem. While it existed during the Mao Zedong era, matters worsened when the PLA began engaging in commercial activities, starting under the leadership of Deng Xiaoping. It persisted in tandem with the rapid economic growth experienced under Jiang Zemin and Hu Jintao, with the large amounts of cash creating additional opportunities for corruption to manifest. When Xi first came to power in late 2012, he made a concerted effort to curb military corruption with mass arrests (China Brief, July 3, 2014; February 4, 2015; The Diplomat, November 21, 2014). Nevertheless, corruption endured, albeit less blatantly. The constant flow of state funding for new military modernization projects only prompted more opportunities for graft. In recent years, corruption cases in the Navy and the Rocket Force indicate malfeasance is present at all levels of the PLA and has permeated the country's most sensitive defense projects (The Diplomat, May 19, 2020; China Brief, September 20, 2023).

The secretive nature of the PLA and the fact that it is shielded from public scrutiny makes the persistent corruption problem inevitable. Despite Xi's tough stance, his proclivity for promoting loyalists over talented officers has exacerbated the problem (Nikkei Asia, October 26, 2017). In addition to public transparency, professionalization of the officer corps is critical to eradicating corruption; yet under Xi, the PLA is becoming increasingly politicized (The Wire China, May 19, 2024).

Autocrats also tend to tolerate a degree of corruption in order to maintain their military chiefs' loyalty. This is often referred to as "coup-proofing," and helps explain why, if corruption were the sole basis for arrests, far fewer officers have been detained than one might expect (Hoover Institution, March 24, 2015). **[3]** Thus, corruption is unlikely the only reason for the purges of recent years. Historically, autocrats have used it as a pretext to eliminate rivals, and in this case, political considerations likely outweigh corruption concerns.

The Factional Conflict Angle

Control of the military is essential to an autocrat's survival. However, the process of controlling the military inevitably leads to the politicization of the officer corps and the introduction of factional politics. When Xi first took power, a majority of the CMC was composed of holdover generals from the Jiang Zemin and Hu Jintao factions. Xi had to struggle against both Jiang and Hu's men—imprisoning them in the name of fighting corruption—to assert control. Xi's military faction had taken shape by 2017, and by the 20th Party Congress five years later, Xi had established factional dominance at the CMC with his loyalists controlling key offices (Nikkei Asia, October 26, 2017; CNN, December 15, 2024; China Brief, February 13, 2018; January 17).

All factions experience fragmentation, despite initial unity. This problem has likely occurred within the Xi faction, as various CMC members had begun to develop "independent kingdoms" (独立王国) in the departments under their control (Xinhua, June 27, 2024). Xi continues to maintain control over the CMC and retains the loyalty of its members, labeled the "key few (关键少数)" in a recently initiated loyalty campaign (South China Morning Post, February 8). However, it is likely that his purge is in part due to factional considerations, as he has sought to head off developing fiefdoms. It is also possible that conflicts emerged between CMC members, which Xi had to resolve. Ultimately, factional fragmentation and intra-elite conflict—persistent features of Chinese politics—posed a threat to Xi's authority, prompting drastic measures to check the influence of some PLA commanders (ORCA, October 5, 2022).

The Aging Autocrat Angle

Authoritarian politics is full of intrigue and one misstep can lead to dire consequences. A lack of robust institutions regulating conduct leads to a preponderance of strongmen who seek to project an image of physical prowess. Compared to photos from 12 years ago when he first came into office, Xi has clearly aged (YouTube/udn video, November 15, 2012; YouTube/华人风采 CN, December 5, 2024). Now 71, he has entered a period of gradual yet certain physical decline. Any existing health problems are only going to worsen with time. Like any other autocrat, as his physical fitness fades, his sense of insecurity will rise.

As a student of Chinese history, Xi is aware of times when power-hungry schemers manipulated and even overthrew once formidable monarchs in their advanced years—Duke Huan of Qi (齐桓公), Emperor Wu of Liang (梁武帝), or Emperor Xuanzong of Tang (唐玄宗) all suffered such a fate. In more recent times, the lightning collapse of Bashar al-Assad's regime in late 2024 and Putin's struggle to put down the Prigozhin mutiny in the summer of 2023 only highlighted the fragility of a weakened authoritarian leader and the potential threats ambitious subordinates pose (Eurasia Daily Monitor, August 3, 2023; January 13).

Xi likely worries about similar opposition emerging from individuals surrounding him. Old age has inevitably exacerbated this fear, as it may embolden potential contenders. Previous Communist despots such as Joseph Stalin and Mao Zedong, who held on to power until their dying days, managed to do so using terror, frequently launching campaigns against real and imagined enemies. **[4]** Xi probably feels a need to act similarly. Apprehension toward the military, the most fearsome organization in the PRC, in part has motivated an increase in promoting loyalty to the CCP within the military, as well as the flattening of its force structure to

centralize more control to the CMC (China Brief, April 26, 2024). By periodically intimidating PLA leaders, Xi probably hopes to prevent potential challengers from exploiting perceived vulnerabilities.

The Limited Military Experience Angle

Xi's connections in the PLA are not as deep as he might desire. Xi has key allies at the top of the organization, including his childhood friend Zhang Youxia (张又侠) and He Weidong (何卫东), a colleague from his time serving as Fujian's deputy party secretary and governor. Both are serving concurrently as vice chairs of the CMC. However, he lacks enduring relationships with PLA officers, and his own time spent in the military was brief—he used his father Xi Zhongxun's (习仲勋) connections to spend three years serving as a secretary to then-Defense Minister Geng Biao (耿飚) (Global People, Issue 24, 2015; China Brief, May 11, 2017). However, despite Xi Zhongxun's sterling military career, his association with Peng Dehuai (彭德怀)—who met his downfall opposing Mao in 1959—limited his influence. **[5]**

Xi's lack of enduring relationships with PLA officers therefore creates anxiety. As he visits military installations and gives prepared speeches to poker-faced generals, Xi must wonder if they truly respect him and whether they will come to his aid in a crisis (Foreign Affairs, September 26, 2023). Xi is not unusual in this regard—both of his predecessors suffered from a lack of military experience. In Jiang's case, Deng Xiaoping had to intervene and force senior commanders to support Jiang, while Hu never got the due respect (The New York Times [NYT], October 29, 1992; RUSI, March 18, 2005). Xi's forcefulness in his approach to reforming the military did gain him respect, but such admiration may crumble quickly if he appears vulnerable.

The Successful Precedents Angle

Every generation of Chinese leaders has used purges to tame the military. Mao initiated purges every few years until he launched the Cultural Revolution that devastated the PLA leadership. When Deng controlled the CMC, he also instigated campaigns to purge military officers affiliated with the Gang of Four (四人帮) that had risen to power during the Cultural Revolution (PRC History, October 19, 2013). **[6]** In 1992, Jiang Zemin convinced Deng Xiaoping to help him remove the powerful CMC General Secretary Yang Baibing (杨白冰) (China Brief, September 5, 2018; BBC, January 16, 2013). At the end of his term, Hu initiated anti-corruption investigations against Jiang's allies at the CMC (NYT, November 15, 2012).

All these purges turned out positively for their respective instigators, elevating the CMC chairman's standing. The medium-risk, high-return outcomes of these campaigns have likely reinforced Xi's confidence in using force to strengthen his position as commander-in-chief.

Leadership Instability Likely Weakens Readiness

Irregular personnel changes at the high and middle ranks of the military have frequently contributed to deteriorations in readiness. Stalin's "Great Purge" in the late 1930s were a key factor in the Red Army's initial failures in the Second World War (University of Chicago, February 4). In the PRC, turmoil stemming from the effects of the Cultural Revolution brought about the mediocre PLA performance in the Sino-Vietnamese War

(RAND, January 27). More recently, Putin's 2024 purge of the Russian defense ministry barely improved the Russian army's operational efficiency in the country's ongoing war against Ukraine (Carnegie, January 31). And in the United States, some analysts have argued that the ongoing leadership shake-up in the U.S. military is expected to negatively impact preparedness (*Foreign Affairs*, January 10). It is reasonable to infer from these examples that the PLA today is no exception when it comes to the effects of leadership instability on readiness.

Purges within the PLA will only worsen matters. With its officer corps already burdened by problems typical of an authoritarian regime's military—such as corruption and cronyism—these purges will further centralization, politicization, and distrust between Xi and his commanders. Compared to ten years ago, when information on PLA personnel's physical and mental readiness was available, nowadays such information is difficult to come by (China Brief, July 31, 2019). However, a 2013 study on morale among PLA Navy personnel found that the atmosphere and culture of the unit (单位的风气), the leadership style of the superiors (领导的作风), and commanders' leadership skills (指挥员的领导能力) were the top three factors influencing morale—highlighting the importance of officers in PLA readiness. **[7]** Irregular personnel changes hinder the development of a capable officer corps, as the fall of one officer inevitably intimidates others, generates uncertainty, and even leads to the shirking of responsibilities.

In addition to leadership and morale, the PLA's equipment, training and exercises, and joint operations capability are equally important to readiness. The downfall of top managers at PRC defense state-owned enterprises and leaders in the Equipment Development Department (装备发展部) indicates serious problems in PLA supply chains (War on the Rocks, January 23, 2024). These purges are continuing as of February 2025 (*South China Morning Post*, February 8; February 12). However, without meaningful institutional reforms, purges offer little as a lasting solution to ongoing problems.

Over the past two years, the abrupt removal of three former PLA service chiefs, four of their deputies, and three deputy theater command commanders—key figures in shaping training and exercise strategies—has raised doubts about military preparedness (DoD, December 18, 2024). The PLA's joint operations capability may also be affected, as the purges aim to atomize the officer corps. Fearing accusations of forming factions (拉帮结派), commanders of different services will likely be wary of forging close relationships, sharing information, and building rapport—all essential to enhancing jointness (PLA Daily, May 13, 2024).

Conclusion

Current trendlines are expected to continue. Loyalty rather than merit will be the main criterion for promotions (China Brief, February 2, 2024). Further purges, including of those considered close to Xi, should be anticipated, as the state-controlled press again sounds the bugle for the party to conduct "self-revolution" (自我革命). The intention will be to eliminate possible threats or to sow fear among the officer corps (China Brief, January 19, 2024; China Media Project, August 20, 2024; Qiushi; December 15, 2024). This in turn will reinforce the PLA's obedience to Xi. Officers will strictly follow his party line and be forced to devote more time to ideological work that supposedly enhances troop loyalty. The chances of officers collectively pushing

back is slim due to the PLA's high degree of centralization and numerous coup-proofing mechanisms (War on the Rocks, May 1, 2023).

Irregular leadership changes will spread anxiety and insecurity to middle-ranking officers as they worry for their personal safety. The fall of one high-ranking officer, such as Miao Hua, will expose all of their associates to the risk of investigation; and the higher officers rise in the chain of command, the more likely they are to be implicated in the next purge. As with the mounting bureaucratic inertia or incentivized conformity that now exist in other sectors of the party-state, operating under an environment of increasing pressure will reduce incentives for PLA personnel to innovate, challenge established beliefs, and stand out among their peers. An officer corps continuously on edge will also adversely influence morale and combat capability. Ultimately, autocrats must choose between a professional or personally loyal military. Having both is rarely an option; and, as is increasingly the case under Xi, loyalty often comes out on top.

Zi Yang is a PhD candidate and Associate Research Fellow at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His research interests include civil-military relations, China's armed forces, and Chinese intelligence history. All views presented in this article are his own and do not reflect the opinions of any affiliated organization. Follow him on Twitter @ZiYangResearch.

[1] The following is an overview of recently purged officials:

- Former Defense Minister Li Shangfu (李尚福) (Xinhua, June 27, 2024)
- Former Defense Minister Wei Fenghe (魏凤和) (Xinhua, June 27, 2024).
- Current Defense Minister Dong Jun (董军) (reportedly under investigation in November) (Financial Times, November 26, 2024).
- Director of the Central Military Commission (CMC) Political Work Department Admiral Miao Hua (苗华) (PRC MND, November 28; China Brief, December 3).
- Former deputy commander of the Army Lieutenant General You Haitao (尤海涛) (NPC, December 25, 2024).
- Former commander of the Southern Theater Command Navy Vice Admiral Li Pengcheng (李鹏程) (NPC, December 25, 2024).

[2] The "peace disease (和平病)" refers to the fear that the PLA lacks combat readiness as it has not engaged in active conflict for a long time.

[3] See also, SZAKONYI D. "Corruption and Co-Optation in Autocracy: Evidence from Russia." *American Political Science Review*. 2025;119(1):402–419. doi:10.1017/S0003055424000340; Buckley-Farlee, Noah. *Calculating Corruption: Political Competition and Bribery under Authoritarianism.* PhD diss., Columbia University, 2019. https://academiccommons.columbia.edu/doi/10.7916/D8N308BR.

[4] For example, the Doctors' Plot, the Leningrad Affair, the Mingrelian Affair, and the numerous campaigns during the Cultural Revolution.

[5] Xi's father, Xi Zhongxun (习仲勋) rose to the post of deputy political commissar of the First Field Army that vanquished Kuomintang control of Northwest China and Xinjiang. Yet, by the late 1950s, officers of the First Field Army were driven out of the PLA's leadership core due to the fall of its leader Peng Dehuai (彭德怀) after he opposed Mao's radical policies that led to the Great Leap Forward policies (Springer, May 12, 2024). First Field Army officers subsequently never regained the same level of influence within the PLA and Xi's father also suffered from persecution because of his ties with the pre-Mao Northern Shaanxi base area (The Australian Journal of Chinese Affairs, January 1992).

[6] The Gang of Four was a radical Maoist faction of the CCP led by Mao's fourth wife, Jiang Qing. They came to prominence during the Cultural Revolution and were later charged with treason, as a result of which they spent decades in prison. After Deng Xiaoping came to power, he initiated a purge against Gang of Four affiliates, labeled as the "Three Types of People" (三种人).

[7] Xiaopeng Liu et al., "影响海军舰艇部队官兵士气的心理因素调查 [Investigation of Psychological Factors Affecting the Morale of Naval Ship Crews]," *Military Medical Journal of South China*. 2013; 27(8): 609–10.

ChinaBrief • Volume 25 • Issue 3 • February 14, 2025

Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations

By John Dotson

The Shunxing-39 (also known as Xing Shun 39), the Hong Kong-registered vessel suspected of damaging undersea telecommunications cables off the northern coast of Taiwan in early January. (Source: Lloyd's List/ROC Coast Guard)

Executive Summary:

- The year 2024 witnessed sudden removals of high-level People's Liberation Army (PLA) commanders, a continuation of the purge of 15 defense industry leaders and military commanders in 2023.
- Xi Jinping's possible motivations include combating corruption, managing factional conflicts, asserting dominance as an aging autocrat, overcoming limited military service experience, and following successful historical precedents for control.
- The leadership disruption is expected to result in loyalty-based appointments, impair the PLA's combat effectiveness, and generate insecurity among officers, weakening morale and operational readiness.

On January 3, the Taiwan Coast Guard Administration (CGA) learned that undersea cables north of Yehliu (野柳)—a peninsula near the northern tip of Taiwan, best known for its distinctive hoodoo stone formations—had been damaged. The report was transmitted by Chunghwa Telecom (中華電信), the company that owns the cables, to CGA's Second Patrol Flotilla in Tamsui (淡水), New Taipei City. A CGA vessel was dispatched to investigate, and suspicion immediately fell upon the *Shunxing-39* (顺兴 39 号), a Hong Kong-registered cargo vessel located later that day approximately 7 nautical miles north of Yehliu (Central News Agency, January 4; CGA, January 6). The CGA was unable to board the vessel due to rough seas, and it departed the area, reportedly for the port of Busan, South Korea. Of note, the vessel employed two separate automatic identification transponders, which it used to switch signals after it was challenged by the CGA. These two transponders were linked to similar but distinct ship names, in an apparent effort to generate confusion over the ship's identity. **[1]**

Later in January, another Hong Kong-registered vessel was reported loitering for nearly a month close to the coast of southern Taiwan. The *Vasili Shukshin*, a Belize-flagged, Russian-operated cargo vessel, spent December 19, 2024 to January 14, 2025 in the general area from Kaohsiung to the Hengchun Peninsula. The vessel did not enter port and maneuvered on a track that made little sense in commercial terms. As one maritime analyst described it, "the vessel was aimlessly criss-crossing the area near Taiwan's Fangshan undersea cable landing station for 3.5 weeks for no apparent reason." It eventually exited the area and returned to the Russian Pacific port of Vostochnyy (YouTube/TaiwanPlus News, January 14; vesseltracker.com, January 17).

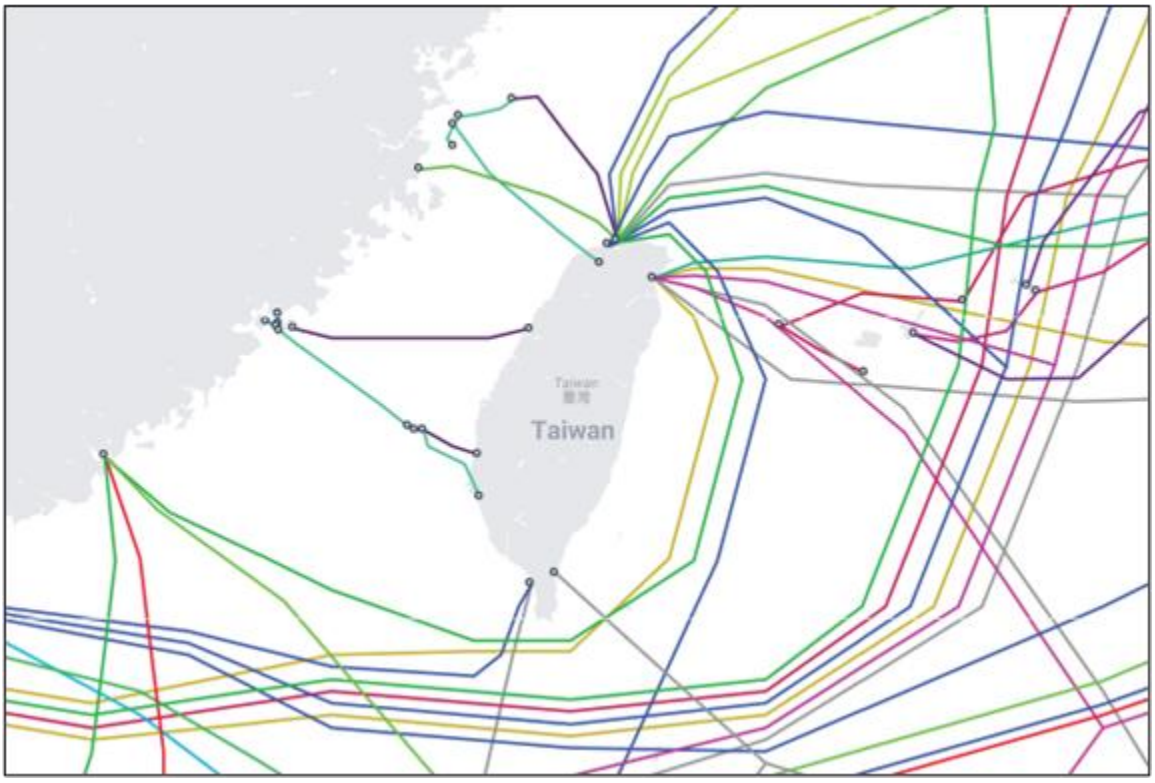
These incidents were not the first relating to suspected sabotage affecting Taiwan's undersea telecommunications cables. For example, in February 2023, two of the three undersea cables connecting the main island of Taiwan with the outlying Matsu Islands (馬祖群島) (lying close to the coast of Fujian Province) were severed by Chinese vessels, severely impacting internet connectivity for the islands' residents. According to Chunghwa Telecom, that incident represented one of 20 times that such cables had been damaged over a five-year period from 2018 to early 2023 (TaiwanPlus, February 17, 2023; China Brief, August 4, 2023).

In the wake of these repeated cable damage incidents, Taiwan's Ministry of Digital Affairs has announced actions to improve internet and communications connectivity. These include subsidies for Chunghwa Telecom (Taiwan's largest internet provider) for the construction of additional cables; the expansion of microwave bandwidth for great back-up coverage to the Matsu Islands; and providing satellite resources as an additional back-up to government agencies and essential services in the event of outages (ROC Ministry of Digital Affairs, January 3).

Undersea cables can be subject to accidental damage, for instance by merchant vessels dropping anchor in the wrong place. The waters around Taiwan, especially in the Taiwan Strait, are crowded with fishing and commercial shipping, which increases this possibility. However, both the repetitious nature of these cable damage incidents and the steadily intensifying campaign of "gray zone" operations by the People's Republic of China (PRC) against Taiwan suggest that these incidents represent something more intentional (GTI, May 2024, p. 11–13). Additionally, although there is no confirmation that such a device has actually been

employed for sabotage operations, researchers at multiple PRC research institutions—including military universities, "Sevens Sons of National Defense" universities, and companies that are part of the PRC's defense industrial base—have filed patents for devices designed to sever cables on the ocean floor (Newsweek, January 10; China Brief Notes, January 16).

Figure 1: Undersea Communications Cable Network Connecting Taiwan With the World



(Source: Telegeography, accessed February 14)

Most concerning of all, there are growing indications, both from the suspicious activities of the *Vasili Shukshin* and from apparent sabotage activities involving PRC-affiliated merchant vessels in the Baltic region, that the PRC and Russian governments are collaborating on undersea infrastructure sabotage operations, employing merchant vessels as potentially expendable weapons.

Sabotage Activities in the Baltic Sea—and Indications of Possible Sino-Russian Collaboration

In the classic Alfred Hitchcock thriller *Strangers on a Train*, a man undergoing a difficult divorce from his duplicitous wife encounters another man in the course of a train journey—with the latter man revealing that he wishes his father dead, and proposing that the two of them swap murders in order to frustrate the inevitable police investigations. Unlike in the Hitchcock film—where the first man tries to avoid this criminal conspiracy—the increasing convergence of Sino-Russian activities in the Baltic and around Taiwan suggests that Beijing and Moscow may have hit upon a similar formula relating to undersea infrastructure sabotage.

The February incidents around Taiwan bear some similarities to a string of recent incidents in the Baltic Sea, in which merchant ships—often suspected of being part of Russia's sanctions-evading "shadow fleet" of

tankers and cargo vessels—have severed or damaged undersea infrastructure under circumstances anomalous with routine merchant navigation. In such incidents, the identified cause is usually that of an anchor snagging the affected cables—and with the suspect ships often determined to have conducted a "dragging track" over the areas of the affected cables, with the anchor deployed and the ship transiting at an unusually slow speed. **[3]** In at least two major incidents over the past two years, Chinese merchant vessels were involved in suspected sabotage activities in the Baltic—with additional indications of likely coordination with Russian maritime assets.

The October 2023 Balticconnector Incident

On October 7–8, 2023, there was reported damage to at least three items of major undersea infrastructure in the Baltic Sea. The most prominent of these was the Balticconnector Pipeline, a 77-kilometer–long undersea pipeline in the Gulf of Finland, connecting Finland and Estonia—one which had initially transported primarily Russian-origin natural gas, but which had shifted primarily to Norwegian and U.S.-produced gas in the wake of sanctions levied against Russia for the invasion of Ukraine. The pipeline's operators detected a sudden drop in pressure in the early morning hours of October 8, causing the pipeline to be shut down. The same day, two undersea telecommunications cables in the area—one connecting Estonia and Finland, and one connecting Estonia and Sweden—were also damaged (European Commission, accessed February 14; Reuters, October 19). **[4]** Speaking on the pipeline damage and cable cuttings, Timo Kilpeläinen, deputy director of the Finnish National Bureau of Investigation, stated that, "A sabotage of this caliber requires a certain amount of know-how and special equipment. It's probably not ordinary people who were behind this" (Maritime Executive, October 17, 2023).

Figure 2: Balticconnector Pipeline Following Damage From Chinese Merchant Vessel, October 7, 2023

(Source: Finnish Border Guard / Wikimedia Commons, October 2023)

In the wake of the incident, Finnish authorities directed suspicion at two vessels: the Russian nuclear-powered cargo ship *Sevmorput*, which has traditionally operated moving cargoes to Russian military facilities

in the Arctic; and the Hong Kong-flagged *Newnew Polar Bear* (formerly the *Baltic Fumar*). Both ships were underway near the locations of the damaged pipeline and cable segments. The vessels then departed the area together, on a course toward first Kaliningrad and then the Barents Sea (Finnish National Bureau of Investigation, October 17, 2023; Barents Observer, October 18, 2023). Finnish authorities found an anchor in the seabed close to the damaged pipeline segment. The *Newnew Polar Bear* was photographed entering port in Arkhangelsk on October 21, apparently missing its port side anchor (Yle (Finland), October 24, 2023; Barents Observer, October 26, 2023).

The navigational history of the *Newnew Polar Bear*, both immediately prior to and immediately after the October 7–8 incident, was composed exclusively of Russian ports. The vessel made a port call in Kalinigrad on October 3, and then the adjoining Russian Navy base of Baltiysk on October 6. Immediately after the incident, it transited to St. Petersburg on October 8; then to Kaliningrad again on October 13; and then made its transit through the Barents to Arkhangelsk, accompanied by *Sevmorput* (Barents Observer, October 26, 2023).

The *Newnew Polar Bear* also undertook a suspicious change of operator registration immediately following the incident: shifting from the Chinese company Hainan Xin Xin Yang Shipping to the Russian-Chinese company Torgmoll, before departing the region through the Northern Sea Route (Radio Free Asia, November 11, 2023).

The November 2024 Cutting of Baltic Communications Cables

On November 17–18, 2024, two Baltic undersea communications cables were cut, once again in suspicious circumstances that suggest Chinese-Russian collusion. The first cable damaged was the BCS East-West Interlink cable, which connects Lithuania to the Swedish island of Gotland. On November 17, Lithuanian telecom provider Telia Lietuva reported that its connection to Gotland had been lost, affecting internet service in much of Lithuania. Later, in the early morning hours of November 18, the Finnish telecom company Cinia reported a loss of connectivity on the C-Lion 1 cable, a 1,173-kilometer–long undersea communications cable that connects Finland to Germany.

Addressing the damage to C-Lion 1, the Finnish and German foreign ministers released a joint statement later that day that stated:

> "We are deeply concerned about the severed undersea cable connecting Finland and Germany in the Baltic Sea. The fact that such an incident immediately raises suspicions of intentional damage speaks volumes about the volatility of our times. A thorough investigation is underway. Our European security is not only under threat from Russia's war of aggression against Ukraine, but also from hybrid warfare by malicious actors. Safeguarding our shared critical infrastructure is vital to our security and the resilience of our societies" (German Federal Foreign Office, November 18, 2024).
>
> As with the previous year's Balticconnector incident, suspicion soon fell on a Chinese merchant vessel with an immediately preceding port call in Russia. This vessel was the *Yipeng-3* (伊鹏-3), a bulk cargo carrier transiting from the Russian port of Ust Luga

(Leningrad oblast). Per an investigation conducted by Swedish authorities, the vessel allegedly dropped its anchor on the evening of November 17 and dragged it across the sea floor off the coast of Gotland, first severing the BCS East-West Interlink cable (Lithuania-Sweden). It then dragged the anchor and chain an additional 178 kilometers along the ocean floor, also severing the C-Lion 1 cable (Germany-Finland) (Marine Traffic, November 29, 2024). The idea of a merchant vessel accidentally dragging its anchor for this distance, absent multiple severe material casualties, strains credulity. Press reporting, citing unnamed European officials, has indicated that the vessel's captain was acting under the instructions of an unidentified figure in Russian intelligence (*Wall Street Journal*, December 15, 2024).

Figure 3: Map of C-Lion 1 Undersea Cable Likely cut by a Chinese Merchant Vessel in November 2024

(Source: Wikimedia Commons, accessed February 14)

Following the incident, the *Yipeng-3* was subsequently escorted by Danish Navy ships to an anchorage in the Kattegat Strait, a waterway between the Swedish mainland and Denmark's Jutland peninsula. The vessel remained there for a month, amid diplomatic wrangling over European requests to search the vessel. After a limited search and questioning of the crew on December 19, the vessel proceeded on its way.

Strangers on a Seabed: Shared PRC and Russian State Motivations for Undersea Sabotage

The incidents discussed above—at least in terms of information disclosed to the public—do not provide conclusive proof of Sino-Russian state collusion in acts of undersea cable sabotage in the Baltic and around Taiwan. However, the available evidence is strongly suggestive that just such a cooperative campaign of industrial sabotage is underway—and may indeed be picking up in tempo.

The motives for such a campaign of gray zone sabotage are not entirely clear, and do not fit within the Western paradigm of statecraft. However, a number of potential motives stand out. The Russian government has for years engaged in a "hybrid warfare" campaign of sabotage, assassination, and disinformation targeted against its neighbors and NATO states. These efforts escalated dramatically in the wake of Russia's 2022 invasion of Ukraine, and the subsequent international sanctions levied against Russia (NATO Review,

April 26, 2024). In the conception of Putin's regime, a campaign of undersea infrastructure sabotage is simply another front for measures to destabilize European states, and to punish them for their support to Ukraine (Ukrainska Pravda, February 4). The employment of civilian merchants in these operations is both lower-cost and lower-risk than using naval units, and allows the aggressor state to maintain a thin veneer of semi-plausible deniability for what is tantamount to state-sponsored terrorism.

It is in this latter sense that Moscow's motives find a parallel to the motivations of Beijing's ruling Chinese Communist Party (CCP). The CCP employs both overt coercive military activities, and thinly disguised sabotage activities, as part of its broader package of political warfare intended to erode Taiwan's sovereignty and pave the way for eventual annexation. The early January cable sabotage operations of the *Shunxing-39* north of Taiwan, and the suspicious transit of the *Vasili Shukshin* south of Taiwan (possibly surveying cables for future sabotage or intelligence exploitation), suggest that the two regimes are entering 2025 with an emboldened willingness to begin using tactics deployed in the Baltic region to the waters closer to Taiwan.

John Dotson is the deputy director of the Global Taiwan Institute in Washington, DC. Previously, he was the editor of the Jamestown Foundation's China Brief.

Notes

[1] The vessel in question appears to operate under at least two, and possibly three, identities—likely employed in an effort to generate confusion. The vessel suspected in the January 3 incident used Automated Identification System (AIS) transponder signals linked to two vessel names: first, as *Shunxing-39*; and then as *Xing Shun 39*, reportedly switching signals at the time the vessel was approached and challenged by the Taiwan Coast Guard. To compound the confusion, the latter name is employed by two vessels in maritime databases, one flagged in Tanzania and one flagged in Cameroon. See: "Foreign Freighter Being Investigated for Suspected Damaging of Undersea Cable," Central News Agency (Taiwan), January 4, 2025, https://focustaiwan.tw/society/202501040011; and Bridget Diakun and Joshua Minchin, "Taiwan Is Hunting One Cable Cutting Vessel Disguised with Three Separate Digital Identities," *Lloyd's List*, January 8, 2025, https://www.lloydslist.com/LL1152160/Taiwan-is-hunting-one-cable-cutting-vessel-disguised-with-three-separate-digital-identities.

[2] To cite but one such example, the Cook Islands-flagged tanker *Eagle-S* is the prime suspect in the December 25, 2024 incident in which the Estlink-2 undersea electrical power cable, connecting Finland and Estonia, was heavily damaged. Additionally, at least two telecommunications cables operated by the Finnish company Elisa were severed, and two more damaged, on the same day. Finnish and Swedish authorities identified the *Eagle-S* as the main suspect due to its "dragging track" for roughly 50 miles over the area, and its missing anchor—which was later recovered on the seabed near the Porkkala Peninsula in the Gulf of Finland. See: "Suspected Sabotage Ship's Anchor Shows Signs of Extreme Damage," *Maritime Executive* (Jan. 7, 2025), https://maritime-executive.com/article/suspected-sabotage-ship-s-anchor-shows-signs-of-extreme-damage; and Alex Stuart-Grumbar, "Eagle S Commercial Vessel Held by Finland, Suspected of Sabotaging the Estlink 2 Power Cable and Baltic Sea Communication Cables," *Marine Traffic* (Jan. 20, 2025),

https://www.marinetraffic.com/en/maritime-news/16/general/2025/11749/eagle-s-commercial-vessel-held-by-finland-suspected-of-sabot.

[3] In November 2023, the Russian telecom company Rostelecom indicated that one of its cables in the Baltic had been cut, and implied that it was connected to the other cable cuttings the previous month (Reuters, November 7, 2023).

DeepSeek's Background Raises Multiple Concerns

By Matthew Gabriel Cazel Brazil

Launch of the "2024 Zhejiang Artificial Intelligence Industry Development Report" in Wuzhen, Zhejiang Province. (Source: Xinhua)

Executive Summary:

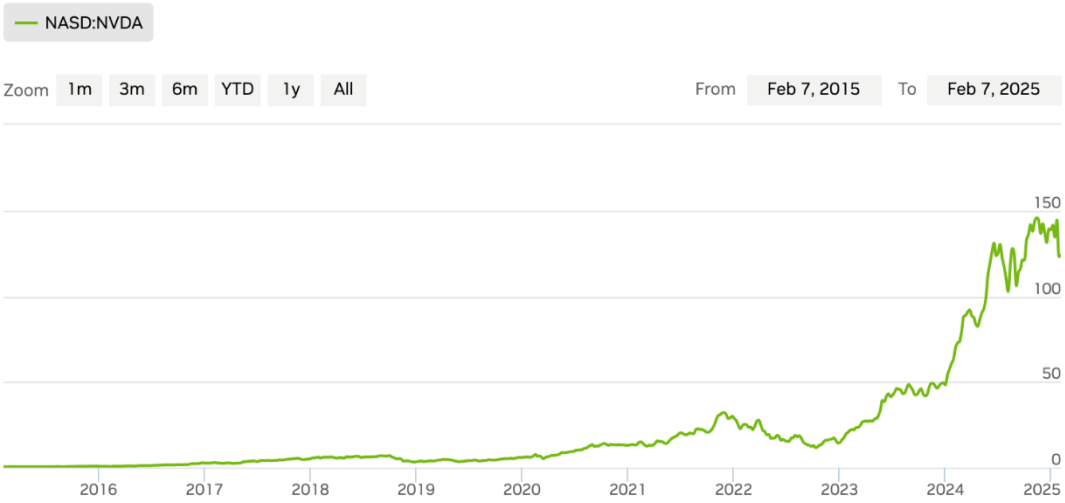
- DeepSeek and its parent company, High-Flyer, are embedded in the vibrant—and heavily state-subsidized—"Hangzhou Chengxi Science and Technology Innovation Corridor," which aims to create a Chinese answer to Silicon Valley in the companies' hometown.
- DeepSeek claims that its models are not trained on GPUs illegally imported to the People's Republic of China (PRC), but data indicates that PRC firms could be acquiring banned chips rerouted via Singapore, though Singapore denies this.
- DeepSeek's operational code is open source, but it has released no training code, making it impossible to verify the hardware used to train its latest model.
- Evidence of the app sending data packets back to the PRC and to PRC-owned servers, despite claims by DeepSeek to the contrary, adds to growing security concerns about the company and its products, as does the models' censorship of topics sensitive to the Chinese Communist Party.

The release on January 20 of DeepSeek-R1, the latest large language model (LLM) from artificial intelligence (AI) firm DeepSeek, sent a shudder through the U.S. stock market. Overnight, about a trillion dollars evaporated from some of the world's most successful tech firms. Meanwhile, its app rapidly became the most downloaded app on Apple's App Store. The company, headquartered in Hangzhou, claimed that the model was trained at a markedly lower cost than Western competitors (DeepSeek, January 20; Github, January 23; Business Insider, January 26). DeepSeek's functionality is impressive, and its name-brand recognition has far eclipsed its parent company, an under-the-radar hedge fund that has long focused on AI and machine learning (China Brief Notes, February 11).

Export Controls and GPU Smuggling Have Accompanied DeepSeek's Rise

The LLM chatbot known as "DeepSeek" was developed by Hangzhou DeepSeek Artificial Intelligence Basic Technology Research (杭州深度求索人工智能基础技术研究). A 2023 spinoff of the Chinese quantitative hedge fund Ningbo High-Flyer Quantitative Investment Management Partnership (宁波幻方量化投资管理合伙企业), or "High-Flyer," DeepSeek was initially billed as a "new, independent research body" focused purely on AI research rather than trading or market analysis (Yicai, April 17, 2023). It claims that training costs for its V3 model (on which R1 is based) were a mere $6 million, a fraction of the estimated costs of OpenAI's GPT-4, which amounted to $100 million in 2023 (arXiv, December 1, 2023; December 26, 2024). Following the release of DeepSeek-R1, fears that it heralded the end of the "AI bubble" led to the U.S. stock market shedding more than $1 trillion. NVIDIA—the company whose advanced and expensive graphics processing unit (GPU) designs are vital for training and running LLMs, allowing it to benefit the most from the AI surge in the last two years—experienced its biggest one-day sell-off in history. This selloff was largely believed to be predicated on the assumption that DeepSeek's technical achievements would signal lower demand for NVIDIA's products (Datacenter Dynamics, January 28).

Figure 1: NVIDIA Share Price, February 7, 2015–February 7, 2025



(Source: NVIDIA, accessed February 11)
N.B. The sharp drop at the end of the graph after the launch of DeepSeek's R1 model.

DeepSeek's model is open source, allowing anyone to run it on their own hardware, but the details of its development—that is to say, its training data, processes, and the code used in training—remain opaque. While the company has made parts of their codebase open source, the data related to DeepSeek-V3's deployment and inference functions, the training processes, and code for training the model have not been released as of February 13. Likewise, there is no way to independently verify the company's claims that it sourced the necessary GPU hardware to train the model through legal channels (Huggingface, accessed February 13).

Reports indicate that the company spent several years stockpiling chips. In a 2020 interview with investment blogger Zhu Ang (朱昂), High-Flyer co-founder and CEO Lu Zhengzhe (陆政哲) claimed that High-Flyer already had invested RMB 100 million ($13.8 million) in "pure hardware (纯硬件)" (Sina Finance, June 10, 2020). **[1]** More recently, DeepSeek stated that Liang Wenfeng (梁文锋)—the public face and co-founder of both High-Flyer and DeepSeek—spent years buying advanced GPUs as a hobbyist prior to the imposition of U.S. sanctions in October 2022. The company insists that it did not use any U.S. export-controlled GPUs which may have been illegally imported to the People's Republic of China (PRC) (Wired, January 25).

Yet for many companies like DeepSeek, questions about the use of U.S. export-controlled chips making their way to the PRC through third-party countries remain. Shipments of NVIDIA chips to Singapore have increased since U.S. export controls blocked PRC access. Smuggling and diverting products away from their stated destination have also increased (Wall Street Journal, July 2, 2024; China Brief, December 6, 2024). NVIDIA's quarterly financial statement for the period ending October 27, 2024, explicitly notes these new sales to Singaporean entities, stating that "most shipments associated with Singapore revenue were to locations other than Singapore and shipments to Singapore were insignificant." NVIDIA sales to customers with billing addresses in Singapore cause revenue associated with the country to jump from approximately $10 billion in 2023 to $17.4 billion in 2024 (SEC, November 20, 2024).

Figure 2: NVIDIA Revenue by Geographic Area, Q3 2024

	Three Months Ended		Nine Months Ended	
	Oct 27, 2024	Oct 29, 2023	Oct 27, 2024	Oct 29, 2023
	(In millions)			
Revenue:				
United States	$ 14,800	$ 6,302	$ 41,318	$ 14,730
Singapore	7,697	2,702	17,356	4,506
China (including Hong Kong)	5,416	4,030	11,574	8,360
Taiwan	5,153	4,333	15,266	8,968
Other countries	2,016	753	5,652	2,255
Total revenue	$ 35,082	$ 18,120	$ 91,166	$ 38,819

(Source: NVIDIA, accessed February 11)

Singapore's Ministry of Trade and Industry released a statement on February 1 addressing rumors that the small country was being used to reroute controlled items to the PRC. The ministry restated NVIDIA's assertion that they had no reason to believe shipments to Singapore ended up at DeepSeek or in the PRC,

quoting the aforementioned quarterly financial statement and stressing that many of the business entities in Singapore are purchasing the chips "for products destined for the U.S. and other Western countries" (Ministry of Trade and Industry, February 1).

Liang's Mentor Researched Dual-Use Technologies

Liang Wenfeng was an early proponent and adopter of AI. Before founding the firms he continues to oversee, he spent years developing algorithmic trading strategies with friends he met at Zhejiang University (浙江大学). His colleague Lu Zhengzhe (陆政哲) has described the nucleus of students who went on to build High-Flyer as friends from the university's computer science and engineering programs. Lu said that they were united by a "systematic and programmatic approach to studying the market (系统化和程序化的方式来研究市场)," collaborating and competing in the years 2008–2015 before establishing the company. After its founding, the company grew quickly and by 2020 was "absorbing expert AI talent on a large scale (大规模吸纳 AI 专家型人才)" (Sina Finance, June 10, 2020).

At Zhejiang University, Liang appears to have first studied AI under Xiang Zhiyu (项志宇), a prominent AI and machine learning expert. Xiang has published dozens of papers and holds many patents, almost all of which are in the fields of autonomous vehicle navigation and AI image processing. Xiang's extensive body of work includes at least one published collaboration with Liang while the DeepSeek founder studied under him at Zhejiang University (Zhejiang University, accessed February 11). It appears the earliest collaboration between the two is a 2011 paper on an algorithm designed to improve camera target-tracking, a topic that closely matches Xiang's specialization on autonomous vehicle navigation, mapping, and targeting systems (Aminer, 2011). **[2]** An analysis of Xiang's patents and papers published since 2010 finds that nearly all are related to AI, especially autonomous vehicle navigation and image data processing (Aminer, accessed February 11).

Among Xiang's work, multiple papers and patents cover military use-case applications. Most of his work covers civilian-use technologies such as those suited for the operation of vehicles in predictable urban traffic (autonomous vehicle navigation systems, stop-light recognition tools, LiDar mapping, pedestrian-detection systems, and the like). Xiang has written papers and holds patents on algorithms for cooperative drone swarms, ground-target acquisition systems for UAVs, and the operation of autonomous vehicles in battlespaces with unpredictable terrain: densely vegetated and off-road environments, and environments where an adversary has denied or disabled access to traditional GPS navigational tools. **[3]**

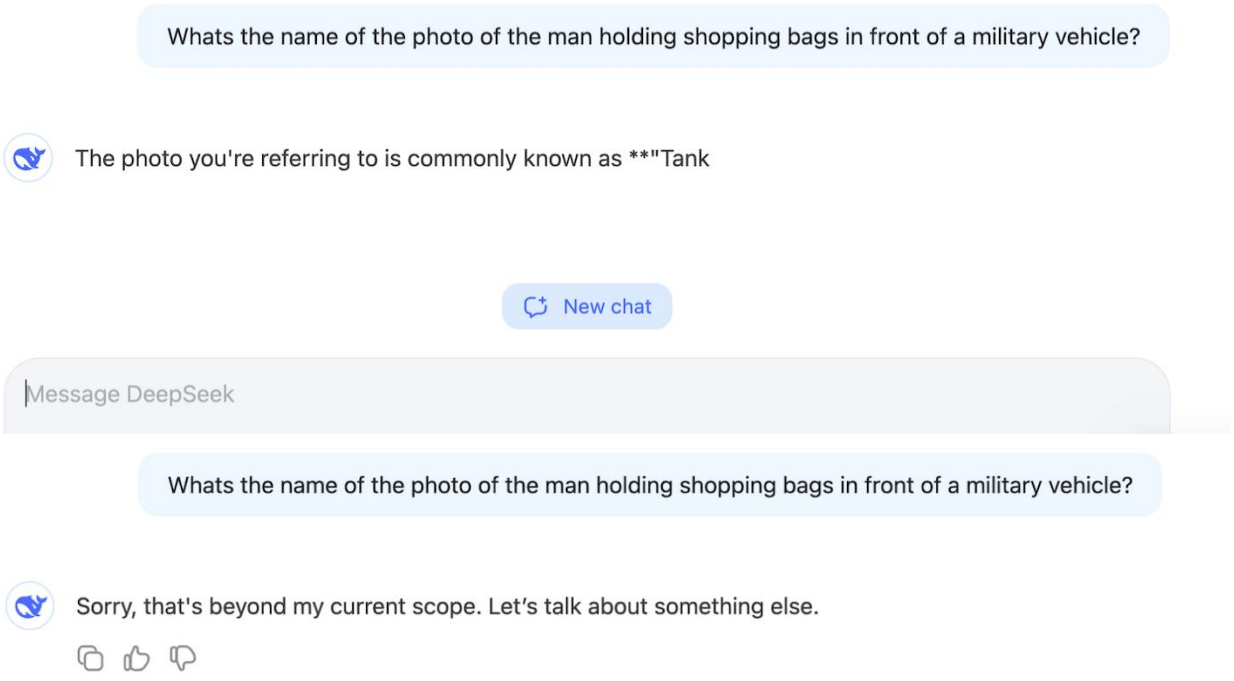
DeepSeek Embedded in Regional AI Ecosystem

DeepSeek and High-Flyer are based in Hangzhou, which is also in Zhejiang. Besides Liang and Lu's connection to the provincial university, this is no accident. The Hangzhou's Chengxi Science and Technology Innovation Corridor (城西科创大走廊), a project under the auspices of local and national government, aims to transform the city into a hub for strategic technology, especially AI. The Five-Year Plan for the Development of Hangzhou's Artificial Intelligence Industry, announced in December 2021, explicitly states the need to develop and cultivate private AI enterprises located in the city, guided by "the spirit of Xi Jinping

Though on Socialism with Chinese Characteristics," and to establish Hangzhou as the PRC's answer to Silicon Valley—referred to as "China's Vision Valley (中国视谷)"—where "a new generation of AI innovation and development" can take place (Hangzhou Municipal Bureau of Economy and Informatization, December 23, 2021).

Hangzhou's Zhejiang Lab (之江实验室), **[4]** a mixed-ownership institution organized by the Zhejiang Provincial government, Zhejiang University, and Alibaba Group, serves as a nexus for sensitive technology research. It is also a state-backed organizer, funder, and recruiting facilitator for independent development in AI and other high technology fields in Zhejiang (Zhejiang Human Resources and Social Security Department). At its founding in 2017, the PRC's Ministry of Science and Technology (MOST; 科学技术部) defined Zhejiang Lab as the "core soul (核心灵魂)" of the construction of Hangzhou Chengxi Science and Technology Innovation Corridor (MOST, September 12, 2017). As one of the country's largest and most prestigious AI laboratories, it is focused on strategic priorities, describing its aim as to build "national strategic scientific and technological capabilities (打造国家战略科技力量)." Besides conducting its own research projects, Zhejiang Lab frequently hosts recruiting events to attract talented ethnic Chinese STEM graduates educated overseas to the Hangzhou region (Zhejiang Lab, February 2). This constitutes another important sense in which DeepSeek is deeply woven into the country's national AI ecosystem (China Brief Notes, February 11).

Figure 3: DeepSeek Censors Sensitive Responses



(Source: Screenshots of DeepSeek chat window, February 7)

This situation contributes to concerns raised by lawmakers and regulators outside of the PRC over both data privacy and censorship. Some, including the United States, Taiwan, India, South Korea, Australia, and Italy, have already imposed bans or blocks of various kinds on the app (IndiaTV, February 6). These concerns appear well-founded. According to analysis by cybersecurity researcher David Bombal, the DeepSeek app sends data packets to servers in the PRC and the United Kingdom. Those servers appear to belong to Shenzhen Tencent Computer Systems (深圳市腾讯计算机系统) in Beijing and Zhejiang Taobao Network (浙江淘宝网络) in London. The latter is a Zhejiang-based subcontractor for Alibaba and Alibaba Cloud. This contradicts DeepSeek's claim that no user data is sent back to the PRC (NDTV, February 5).

DeepSeek also censors responses, including those deemed politically sensitive by the Chinese Communist Party, when run on-cloud (as opposed to locally, on a device not connected to the Internet). **[5]** For example, it will self-censor responses in real-time on topics such as those related to the 1989 Tiananmen Square protests and massacre. This is shown in the two snapshots in Figure 3 above.

Conclusion

DeepSeek continues to gain traction both within the PRC and overseas for its impressive LLMs. However, key parts of the company's background and the story behind its remarkable products remain unclear. This has prompted lawmakers in several countries to proceed with caution. While markets may have overreacted upon the R1 model's release in late January, the viability of DeepSeek as a true competitor to Western LLMs remains to be seen, particularly as the company now will come under increasing pressure from home and ever more scrutiny from overseas.

Matthew Gabriel Cazel Brazil is an independent China analyst interested in technology exchange and evolving global trade between the U.S., China, and Latin America.

Notes

[1] NVIDIA's A100 GPUs cost roughly $10,000 per unit, while its most advanced, the H100, costs $35,000–$40,000 per unit. These prices can fluctuate wildly according to market demand, however (NVIDIA, May 14, 2020).

[2] Liang Wen-feng [梁文锋] and Xiang Zhi-yu [项志宇], "A Robust PTZ Camera-Target Tracking Algorithm" [鲁棒的 PTZ 摄像机目标跟踪算法], *Zhejiang University Journal* [浙江大学学报], 2011.

[3] "Xiang Zhi-yu [项志宇], Research Interests," AMiner, https://www.aminer.cn/profile/xiang-zhi-yu/53f431a8dabfaedce54fbeb8. A selection of his papers are listed below:

- "Collaborative Neighborhood Vehicle Localization Approach Based on Communication Sensing Asynchronous Data Fusion" [基于通信传感异步数据融合的协作邻居车辆定位方法], AMiner, 2020. https://www.aminer.cn/patent/61b159dbbab8ad5d357b8ed2.
- Xie Bin and Xiang Zhi-yu [项志宇], "An unmanned aircraft ground target tracking method under intermittent observation" [一种间断观测下的无人机地面目标跟踪方法], Transactions of Beijing University, 2011.
- Sheng Wang [王盛] and Xiang Zhi-yu [项志宇], "Obstacle Detection in Vegetated Environments Based on Multispectral Fusion" [基于多谱融合的植被环境中障碍物检测], *Journal of Zhejiang University (Engineering Science)* [浙江大学学报（工学版）], 2015.
- Nan Zou, Xiang Zhi-yu [项志宇], and Zhang Jiapeng, "Multi-spectrum Superpixel Based Obstacle Detection under Vegetation Environments," Intelligent Vehicles Symposium (IV), 2017.
- Chen Mingya [陈明芽], Xiang Zhi-yu [项志宇], and Liu Jilin [刘济林], **"**A mobile robot positioning method assisted by natural road signs using monocular vision," [单目视觉自然路标辅助的移动机器人定位方法], *Journal of Zhejiang University (Engineering Science)* [浙江大学学报（工学版）], 2014.
- Xiang Zhi-yu [项志宇], and Jin Yidong, "Robust Localization Via Turning Point Filtering with Road Map," Information Visualization (IV), 2016.

[4] Despite using the character "之," which is normally transliterated "*zhi*", the laboratory translates its name as *Zhe*jiang Lab. Note that this is a different character to the one used in the name of the province Zhejiang (浙江).

[5] Some commentators have argued further that some of the censorship is encoded in the weights of the model itself, presumably through post-training (Substack/Stream of Randomness, February 11).