EuroHub4Sino

European Hub
for Contemporary China

*August 2026*

# Open by Design, Exposed by Default: Data Security and the Strategic Challenge of PLA Intelligentised Warfare

*by Maud Descamps*

Funded by
the European Union

https://doi.org/10.31175/eh4s.r2kw

## KEY TAKEAWAYS

- What counts as relevant is being redefined by intelligentisation, where data quality determines AI effectiveness, making peacetime civilian data acquisition a form of military preparation.
- The establishment of ISF in April 2024 institutionalised the doctrinal shift of information gathering into intelligentisation.
- MCF creates legal pathways for access to civilian capabilities and information, rather than implying automatic espionage or data transfer.
- There is an aggregation problem as individual datasets may appear innocuous or commercially oriented, yet their combination can generate strategic value by enabling more comprehensive profiling, inference, targeting, or AI training.
- The EU's principal gap is one of integration rather than absence: the EU already possesses instruments addressing cybersecurity, data protection, AI, investment screening, and research security, but these frameworks are not systematically connected around the cumulative military value that data can acquire through aggregation.

***Keywords***

*AI*

*PLA Tech*

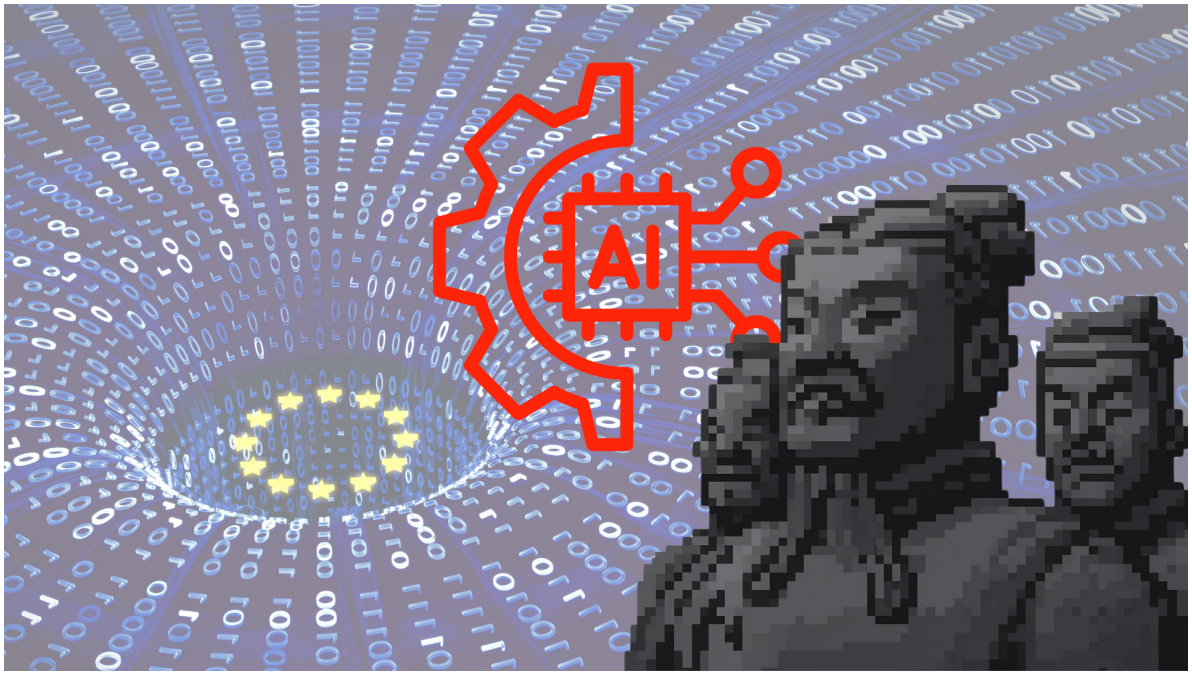
*MCF*

*PLA doctrine*

*Military-Civil Fusion*

*EU data*

*Cybersecurity*




## Introduction

China is undergoing a qualitative transformation in how it understands military power. The 2019 defence white paper marked the official elevation of intelligentised warfare (智能化战争, zhìnéng huà zhànzhēng) in China's defence discourse, describing it as an emerging form of warfare driven by advances in AI, big data, cloud computing and other technologies. Its current modernisation phase, intelligentisation, treats data not as a by-product of military activity but as a strategic resource essential for AI-enabled decision-making. The April 2024 creation of the Information Support Force (ISF) reflects this shift by placing data integration and information support at the centre of joint operations. By overseeing the networks, communications, and information infrastructure through which data is collected and shared across the PLA (Pleople's Liberation Army), the ISF provides a key institutional foundation for intelligentised warfare.

For Europe, the challenge extends beyond traditional defence concerns. China's Military-Civil Fusion (MCF) framework[1] deliberately links civilian and military technological ecosystems, allowing commercially acquired data, research outputs, and infrastructure information to contribute to broader national-security objectives. Individually, datasets such as geospatial information, logistics records, telecommunications metadata, or industrial data may appear benign. Aggregated and analysed at scale, however, they can reveal infrastructure dependencies, supply-chain vulnerabilities, and operational patterns with potential military value.

This challenge is becoming increasingly relevant as the European Union accelerates defence investment under initiatives such as Readiness 2030 and ReArm Europe. While these

efforts seek to strengthen military capabilities, they also increase reliance on AI, cloud infrastructure, telecommunications networks, and digitally enabled civilian systems. The key question is therefore not only whether Europe is strengthening its military capabilities, but whether the civilian data ecosystems underpinning those capabilities are receiving comparable security attention.

Existing EU instruments addressing cybersecurity, data protection, investment screening, research security, and critical infrastructure provide important safeguards. Yet they do not consistently assess the cumulative military significance that can emerge when civilian datasets are aggregated across sectors. This brief identifies that gap and proposes policy responses.

## PLA Intelligentised Warfare

### Doctrinal Shift

PLA modernisation has followed a three-phase trajectory: mechanisation, informatisation, and intelligentisation.[2] Mechanisation focused on modern platforms and weapons. Informatisation connected those systems through digital networks, communications systems, and information-sharing architectures. Intelligentisation[3] goes a step further by transforming information into decision advantage through artificial intelligence and large-scale data integration.

Under this approach, information generated by satellites, unmanned systems, radar, cyber operations, electronic warfare assets, and other sensors is integrated into shared data architectures. The purpose is not merely to connect different systems but to create a continuously updated operational picture that supports faster and more informed decision-making. AI-enabled tools can assist commanders by identifying patterns, prioritising threats, evaluating courses of action, and coordinating operations across domains.

The U.S. Department of Defense's 2024[4] assessment similarly notes that the PLA views information superiority as a prerequisite for successful military campaigns and is pursuing next-generation capabilities based on AI, big data, quantum computing, and other emerging technologies. Military effectiveness consequently depends increasingly on access to large volumes of reliable and timely data.  The operational logic can be represented as a causal chain[5]:

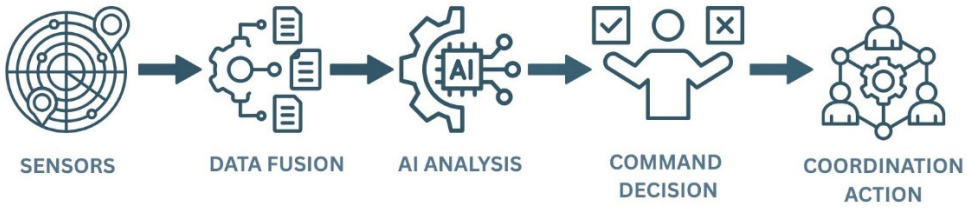



*Figure 1 Author's illustration based on U.S. Department of Defense (2024), and Center for Security and Emerging Technology (2026)*

Intelligentisation places greater emphasis on common data architectures capable of integrating information generated across different services and operational domains.[6] The objective is to move beyond information sharing between systems towards the continuous fusion of information into a machine-readable battlespace picture from which commanders, and increasingly automated systems, can derive decisions. AI models are consequently dependent not only on computing power but also on the quantity, diversity, timeliness, and reliability of the data used to train and deploy[7] them.

Thus, Intelligentisation represents an infrastructure challenge as much as a weapons-development effort. AI-enabled military systems require sensors, communications networks, cloud computing resources, databases, and data-management structures capable of supporting continuous information fusion. China's 15th Five-Year Plan (2026–2030) reflects this logic by linking the development of information systems, data resources, and intelligentised military capabilities within a broader framework[8] of national strategic integration. This institutional approach extends beyond the PLA itself, linking military requirements to China's wider technological, industrial, and data ecosystem through mechanisms associated with military-civil fusion (MCF)[9].

The strategic consequence is significant. Data is no longer simply generated through military operations; it has become a critical input that must be acquired, managed, and protected before conflict occurs.

## Institutionalisation of Data Warfare

The clearest evidence that intelligentisation is operational is that it has moved from doctrine into military organisation, as seen with the PLA's April 2024 restructuring[10] of its information-support architecture. On 19 April 2024, Beijing dissolved the Strategic Support Force (SSF), which had unified space, cyber, and information operations since 2015. The principal functions of SSF have been placed under three separate Central Military Commissions (CMC): the Aerospace Force (ASF), responsible for space-based military capabilities; Cyberspace Force (CSF), dedicated to network warfare and offensive cyber operations; and

the Information Support Force (ISF)[11]. The ISF is responsible for providing information support, including the networks, communications, and information infrastructure required for joint operations. The reform is significant because it gives information support an institutional position at the centre of joint operations. Thus, the organisational change reflects a broader shift in how the PLA intends to fight: information must be collected, transmitted, integrated, and made available across the force quickly enough to support joint operations.

**Organisational Structure of the Military Forces in China**[12]

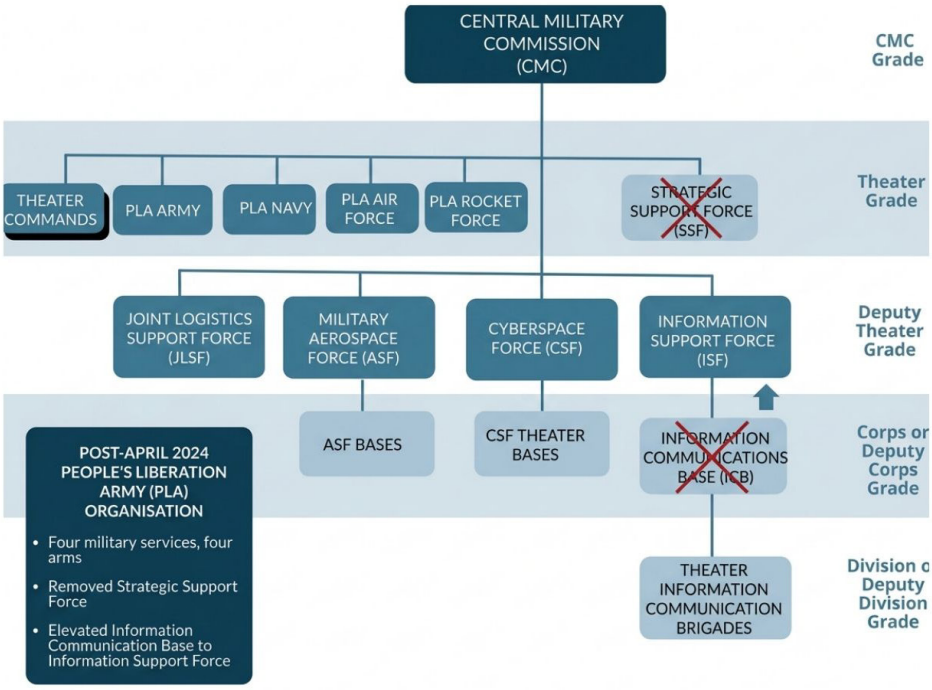



*Figure 2 Author's illustration based on U.S. Department of Defense (2024), CNA (2024), Jamestown Foundation (2024), and Cyberspace Administration of China (2017)*

The importance of the ISF extends beyond providing communications infrastructure. Intelligentised warfare depends on the ability to collect, transmit, integrate, and distribute large volumes of data rapidly across the force. AI systems depend on sufficiently large, relevant, and reliable datasets to support effective battlefield assessment. The ISF contributes to the networked information environment through which data generated by sensors, units, and command systems can be made available for analysis and operational decision-making. The April 2024 reform should consequently be understood not simply as an administrative reorganisation, but as an institutional recognition that the effective exploitation of information has become a core requirement of joint warfare.

This also changes the military significance of data acquired before conflict begins. If the quality of training data directly affects[13] the performance of intelligent algorithms, then

data relevant to military AI can acquire value long before it is used operationally. Commercial, industrial, scientific, infrastructure, and telecommunications datasets can potentially contribute to models, simulations, geographic understanding, or assessments of an adversary's capabilities and vulnerabilities. The relevant question is therefore not whether a dataset is explicitly military, but whether it can improve the PLA's ability to understand, model, or operate within the battlespace.

### MCF: Civilian Data Pipeline as Military Resource

The connection between China's civilian technological ecosystem and military modernisation is reinforced by the broader framework of Military-Civil Fusion (MCF). MCF is a state-led strategy for integrating civilian and defence capabilities, encouraging the sharing and coordinated development of technologies, infrastructure, talent, research, and industrial capabilities that can contribute to national defence[14].

Two legal provisions are particularly relevant to the potential extraterritorial implications of this framework. The 2015 National Security Law[15] adopts a broad conception of national security encompassing political, economic, military, cultural, social, and other domains. The 2017 National Intelligence Law[16] further provides, in Article 7, that "any organisation or citizen shall support, assist, and cooperate with state intelligence work." Together, these provisions illustrate how Chinese law can connect civilian entities and activities to national-security and intelligence objectives. They do not mean that every Chinese company is automatically an agent of the state or that all civilian data is accessible to intelligence authorities. Rather, they highlight the importance of considering the legal and institutional environment[17] in which Chinese entities operate when assessing access to strategically significant data, infrastructure, technologies, or research.

This distinction is particularly important in Europe. A Chinese company, research institution, or technology provider does not need to be formally designated as a defence contractor for information obtained through commercial or research activities to have potential strategic value. Access to European industrial processes, infrastructure information, geospatial datasets, telecommunications systems, supply-chain information, or dual-use research can contribute to China's broader technological and intelligence ecosystem. The potential security problem lies not only in the transfer of explicitly military technology, but also in the aggregation of otherwise civilian information that can become militarily relevant when combined with other datasets and capabilities.[18]

## Europe's Exposure

### Research and Technology Partnerships

The exposure operates at several levels simultaneously. Research partnerships can provide access to datasets, including dual-use data with potential military applications in ar-

eas such as materials science, autonomous systems, quantum technologies, and artificial intelligence. They can also provide methodologies, technical expertise, models, and tacit knowledge that may be difficult to acquire through conventional technology transfers. Participation in European research networks can additionally create relationships and institutional knowledge that facilitate future access to expertise and infrastructure. Research-security assessments nevertheless remain uneven[19] across Member States.

This situation is not limited to EU research programmes. Member States are also pursuing bilateral cooperation with China in strategically relevant technologies. Slovakia provides a good illustration: during President Peter Pellegrini's July 2026 visit[20] to Beijing, cooperation in digital and emerging technologies featured alongside broader economic and investment ties. Such cooperation is not inherently problematic and does not imply that participating Slovak entities are acting on behalf of the Chinese state. It nevertheless illustrates the policy challenge: individual technology partnerships may be legitimate, while their cumulative contribution to European technological and data exposure is harder to assess.

## Infrastructure and Data

The more strategically significant exposure is infrastructural. European military capabilities increasingly depend on civilian digital and physical infrastructure, while the operation of this infrastructure generates data that may have military and intelligence value.

Three areas are particularly relevant: telecommunications, cloud infrastructure, and logistics. Telecommunications infrastructure generates metadata on traffic patterns, geographic distributions of activity, and network architecture. Huawei equipment remains present in parts of several European telecommunications networks, despite EU efforts to restrict high-risk suppliers through measures such as the 5G cybersecurity toolbox[21]. Aggregated over time, telecommunications data can provide insights into communications dependencies and vulnerabilities.

Cloud and data processing present a different but related challenge. European dependence on a small number of major cloud providers raises questions about who operates the infrastructure through which strategically sensitive datasets are stored, processed, and aggregated. Three US companies account for approximately 65 percent[22] of the European cloud services market, illustrating the concentration of infrastructure on which European institutions and other strategic actors increasingly depend. The significance of cloud infrastructure lies not only in data storage but also in the ability to process information across systems and datasets, potentially revealing patterns that are not apparent in individual datasets.

Ports, logistics, and industrial systems generate another important category of data. Chinese state-owned shipping interests have established significant positions in European port infrastructure, most prominently through COSCO[23] Shipping's investment in the Port

of Piraeus. Port and logistics systems generate continuous information on cargo flows, supply-chain dependencies, infrastructure use, and transportation patterns. Where civilian infrastructure also supports military mobility, these data streams could provide insights into military logistics and force movements. Industrial and smart-city systems similarly generate sensor and operational data which, when collected across sites and over time, can contribute to a broader picture of infrastructure dependencies and vulnerabilities.

No single dataset is necessarily sensitive in isolation. Their aggregation, however, can reveal infrastructure dependencies, logistical patterns, and potential vulnerabilities that are difficult to identify from individual datasets.

### Where Existing Security Instruments Fall Short

The EU is not starting from scratch and possesses a substantial set of security instruments[24], including investment screening mechanisms, cybersecurity regulations, critical-infrastructure protections, research-security initiatives, and economic-security measures. The gap lies instead in how these instruments connect. Existing frameworks generally assess specific risks, sectors, transactions, or systems. They are less suited to identifying the cumulative military value that can emerge when otherwise legitimate access to civilian datasets, infrastructure, research, and technologies is combined over time.

This limitation matters because intelligentised warfare relies precisely on the aggregation of information. Telecommunications metadata, logistics information, industrial production data, infrastructure records, and research outputs may appear predominantly civilian when assessed individually. Analysed collectively, however, they can provide insights into military mobility, supply-chain resilience, infrastructure vulnerabilities, and force-generation capacity. The strategic significance of a dataset may therefore depend less on its classification or original purpose than on what can be inferred when it is combined with other information.

The policy gap is therefore one of integration and strategic assessment rather than regulatory absence. Existing EU instruments provide important entry points, but they do not yet consistently assess whether access obtained through separate commercial, research, technological, or infrastructural relationships can cumulatively contribute to a foreign state's military capabilities. This is particularly relevant in the Chinese context, where Military-Civil Fusion seeks to connect civilian technological, industrial, scientific, and information resources with broader national-security objectives.

## Conclusion: Policy Implications

The challenge posed by China's intelligentisation strategy is not primarily one of espionage, cyber intrusion, or illicit technology transfer. Rather, it stems from the growing military value of information acquired legally through commercial, research, and infrastruc-

tural engagement and becoming strategically significant when aggregated at scale. The creation of the PLA's Information Support Force illustrates that China increasingly treats data as a military resource, while Military-Civil Fusion creates mechanisms connecting civilian technological, industrial, scientific, and information resources to national-security objectives.

This has important implications for Europe. The EU already possesses extensive instruments addressing cybersecurity, investment screening, critical infrastructure, economic security, and research security. The problem is therefore not simply a lack of regulation, but how risk is assessed. Existing frameworks tend to evaluate datasets, infrastructures, investments, or research relationships separately, while the strategic advantage sought through intelligentised warfare can emerge from their combination.

European policymakers should therefore place greater emphasis on the cumulative strategic value of data. Risk assessments should consider not only whether individual datasets are classified, personal, or explicitly military, but what could be inferred when information from different sources is combined. Existing mechanisms can be adapted to account for how civilian data access may contribute to military capability across sectors and Member States.

The same logic should apply to foreign engagement. Where organisations operate within legal or institutional frameworks connecting civilian activities to Chinese state intelligence or defence objectives, this context should inform assessments of strategically significant infrastructure, research partnerships, technologies, and datasets. Such linkages should not automatically determine the outcome of an investment or partnership, but they should be treated as a relevant factor in assessing strategic exposure.

The objective is not to close European data ecosystems or restrict legitimate engagement with China. It is to ensure that openness does not create strategic dependencies that become visible only after they have formed. In an era of intelligentised warfare, Europe must therefore learn to identify not only sensitive data, but also when ordinary data becomes strategically consequential through aggregation.

**[1]** Zhu Y., "From Military Dominance to Military-Civil Fusion: China's National Defence in the Semiconductor Industry," EuroHub4Sino Policy paper 2026/13, August 4, 2026, accessed August 18, 2026, https://reddragon1949.com/chinas-informatization-%e4%b8%ad%e5%9c%8b%e4%bf%a1%e6%81%af%e5%8c%96/military-big-data-driving-future-chinese-military-transformation/ ; see also Descamps M., Yuan J?, Zhu Y., "Military-civil Fusion is a key Chinese Strategy with long-term Implications: An Interview with Jingdong Yuan and Yifei Zhu," ISDP Expert Take, April 2025, accessed June 5, 2026, https://www.isdp.eu/publication/military-civil-fusion-is-a-key-chinese-strategy-with-long-term-implications/?utm_source=chatgpt.com

**[2]** U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," Annual Report to Congress, 2024, p.25, accessed on June, 2026, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF; see also "习近平在中国共产党第十九次全国代表大会上的报告," Report at the 19th National Congress of the Communist Party, October 18, 2017, Accessed on June 5, 2026, https://www.cac.gov.cn/2017-10/26/c_1121867641.htm.

**[3]** Ibid.

**[4]** U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," Annual Report to Congress, 2024, p.VIII, accessed June, 2026, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

**[5]** Ibid; see also Probasco E., Bresnick S., McFaul C., "China's Military AI Wish List," CSET, Issue Brief, February 2026, accessed June 10, 2026, https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Military-AI-Wish-List.pdf.

**[6]** Ibid.

**[7]** « Military Big Data : Driving Future Chinese Military Transformation," Interview Third Military Big Data Forum, Red Dragon 1949, January 31, 2026, accessed July 2, 2026, https://reddragon1949.com/chinas-informatization-%e4%b8%ad%e5%9c%8b%e4%bf%a1%e6%81%af%e5%8c%96/military-big-data-driving-future-chinese-military-transformation/; see also Wang H., Lei S., "第三届"军事大数据论坛" ," September 16, 2021, accessed July 2, 2026, http://military.china.com.cn/2021-09/16/content_77757778.htm.

**[8]** "15th FYP Explorer," accessed July 2, 2026, https://chinafyp.com/.

**[9]** The State Council – The People's Republic of China, "Full text: Recommendations of the Central Committee of the Communist Party of China for Formulating the 15th Five-Year Plan for National Economic and Social Development," October 28, 2025, accessed May 25, 2026, https://english.www.gov.cn/news/202510/28/content_WS6900adb9c6d00ca5f9a07216.html.

**[10]** U.S. Department of Defense, "Fact Sheet – 2024 China Military Report," Accessed July 20, 2026, https://media.defense.gov/2024/Dec/18/2003615417/-1/-1/0/2024-CMPR-FACT-SHEET.PDF.

**[11]** Mulvaney B. S., "The PLA's New Information Support Force," Air University (AU), April

22, 2024, accessed August 4, 2026, https://www.airuniversity.af.edu/CASI/Display/Article/3749754/the-plas-new-information-support-force/.

**[12]** U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," Annual Report to Congress, 2024, p.25, accessed on June, 2026, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF; see also Cyberspace Administration of China "习近平在中国共产党第十九次全国代表大会上的报告," Report at the 19th National Congress of the Communist Party, October 18, 2017, Accessed on June 5, 2026, https://www.cac.gov.cn/2017-10/26/c_1121867641.htm.; see also "PLA Update," CNA, Issue 20, April 20, 2024, accessed June 5, 2026, https://www.cna.org/Newsletters/PLA%20Update/Issue-20/PLA-Update-Issue-20-April-30-2024.pdf; see also "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025," U.S. Department of Defense, 2025 Annual Report to Congress: Military and Security Developments Involving the People's Republic of China; see also Dahm J. M., "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force," Jamestown Foundation, China Brief, Volume 24 Issue 9, April 26, 2024, accessed June 5, 2026, https://jamestown.org/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/.

**[13]** Bai X., Li X., "Chinese Military Building a Solid Data Foundation for Victory in the Intelligent Battlefield," PLA Doctrinal Analysis, Red Dragon 1949, January 16, 2025, accessed June 20, 2026 https://reddragon1949.com/chinese-military-informatization/%e4%b8%ad%e5%9c%8b%e8%a7%a3%e6%94%be%e8%bb%8d%e6%95%98%e4%ba%8b%e6%88%b0%e7%88%ad/chinese-military-building-a-solid-data-foundation-for-victory-in-the-intelligent-battlefield/.

**[14]** National Energy Administration, "国务院办公厅关于推动国防科技工业军民融合深度发展的意见," December 25, 2017, accessed June 18, 2026, https://www.nea.gov.cn/2017-12/25/c_136849980.htm.

**[15]** "National Security Law of China (2015)," China Justice Observer, July 1, 2015, accessed August 10, 2026, https://www.chinajusticeobserver.com/law/x/national-security-law-20150701.

**[16]** National People's Congress of the People's Republic of China, "中华人民共和国国家情报法," June 27, 2017, accessed July 14, 2026, http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055873.htm.

**[17]** Descamps M., « China's Cybersecurity Legislation: A Paper Tiger or an Institutionalized Theft?," ISDP Focus Asia, May 2020, pp. 2- 3, accessed July 14, 2026, https://www.isdp.eu/publication/chinas-cybersecurity-legislation-paper-tiger-institutionalized-theft/.

**[18]** Swanström N., Zhu, Yi., "China's Quest for Military Technology through Foreign and Civil Sources: Strategic Trends under Xi Jinping and Tactical Adjustments amid Geopolitical Challenges," EuroHub4Sino Policy Paper 2024/7, July 2024, https://doi.org/10.31175/eh4s.2014.07.

**[19]** European Commission Directorate-General for Research and Innovation, "Research Se-

curity Monitor 2025 – Raising awareness and building resilience," Staff Working Document, December 2025, p.10, accessed July 24, 2026, https://european-research-area.ec.europa.eu/documents/research-security-monitor-2025.
**[20]** "President Xi Jinping Holds Talks with President of Slovakia Peter Pellegrini," Ministry of Foreign Affairs – People's Republic of China, July 28, 2026, accessed August 10, 2026, https://www.fmprc.gov.cn/eng/xw/zyxw/202607/t20260728_11993771.html.
**[21]** European Commission, "Communication from the Commission: Implementation of the 5G cybersecurity Toolbox," June 15, 2023, accessed August 1, 2026, https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox.
**[22]** Perugini M., "Europe's Ungoverned Space: Military AI and the Autonomy That Cannot Be Bought," VoxEU, June 22, 2026, accessed August 4, 2026, https://cepr.org/voxeu/columns/europes-ungoverned-space-military-ai-and-autonomy-cannot-be-bought.
**[23]** Saul J., Souliotis Y., Maltezou R., "Greece examines impact of US blacklisting of Piraeus port owner COSCO," Reuters, January 10, 2025, accessed July 14, 2026, https://www.reuters.com/world/greece-examines-impact-us-blacklisting-piraeus-port-owner-cosco-sources-2025-01-10/.
**[24]** European Commission, "Investing in Europe's Prosperity," November 2024, accessed July 20, 2026, https://ec.europa.eu/commission/presscorner/api/files/attachment/879952/5%20Investing%20in%20Europe's%20prosperity.pdf.




Funded by
the European Union

The project "European Hub for Contemporary China (EuroHub4Sino)" has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement number 101131737.

UK participants in Horizon Europe Project European Hub for Contemporary China are supported by UKRI grant numbers 10108183 and 10108749.

Funded by the European Union. Views and opinions expressed are however those of the authors) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.