“Smartphones on Wheels”: Connected Cars and the EU’s Cybersecurity

Paulina Uznańska *

December 2025

* *Paulina Uznańska is an analyst in the China Team, focusing on the PRC’s technology policy and EU–China relations. Paulina is also a PhD candidate at the University of Cologne and the University of Warsaw, specialising in Chinese law. Paulina is a co-founder of the Polish Research Centre for Law and Economy of China at the University of Warsaw and a fellow of the International Visegrad Fund and the Polish National Agency for Academic Exchange. She was a visiting scholar at National Taiwan University and National Chengchi University. She co-edits monographs in Chinese ("New Technologies and Law 新科技与法律", Scholar 2022) and translates from Mandarin ("China-Central and Eastern Europe. A History of Literary Interactions," Dialog 2020)*

This policy paper was produced within the Think Visegrad in Brussels Fellowship programme. In the first half of 2016, eight think-tanks from the Visegrad Group that have been cooperating in the Think Visegrad platform, agreed on the idea proposed by the EUROPEUM Institute for European Policy, to create a common representation office in Brussels. The main motivation for it is the need to encourage debate on issues of common interest to the EU and the V4 and explain the positions of the V4 to a wide audience. Think Visegrad in Brussels would like to project an image of constructive partners, to explain the dynamics of the debates within our regions and to highlight our active contributions to EU policy-making. For more information about Think Visegrad and its members visit www.think.visegradfund.org.

Contents

Introduction

Chinese connected vehicles (智能网联汽车) are rapidly proliferating on European roads, marking a structural shift in the EU's automotive and digital landscape. In 2025, Chinese automakers sold about 810,000 vehicles in Europe — up 99% year-on-year — lifting their market share to 6.1%.[1] In August 2025, they had even surpassed prominent European manufacturers in the regional market, including Audi and Renault.[2] Among the more than 40 brands originating from China, the most prevalent are MG, BYD, Jaecoo, Omoda, and Leapmotor.[3]

The growing popularity of Chinese connected vehicles has intensified concerns in Europe over cybersecurity risks, including their potential use for surveillance, espionage, and cyberattacks.[4] These debates often reference regulatory responses and risk assessments developed in other countries, particularly the United States.[5] However, it is China that has developed one of the world's most extensive regulatory and technical standardisation frameworks for connected vehicles.

This paper offers insights into how the Chinese authorities conceptualise the cybersecurity implications of connected vehicles. This study draws on Mandarin-language documents published by central and local Chinese institutions, including ministries, regulatory authorities, standardisation bodies, and municipal administrations. It also sets out recommendations based on the author's interviews with representatives of EU institutions. This paper will be followed by a comprehensive report on the same topic issued by the Centre for Eastern Studies (OSW).

[1] B. Anderson, *One in 10 New Cars Sold in Europe Last Month Was Chinese*, CarScoops, 22 January 2026, https://www.carscoops.com/2026/01/chinese-car-sales-europe-2025-record-growth/
[2] *Chinese car brands outsell Renault in Europe in August*, JATO, 23 September 2025, https://www.jato.com/resources/media-and-press-releases/chinese-car-brands-outsell-renault-in-europe-in-august
[3] A. Parodi, *Europe's plug-in hybrid boom helps Chinese carmakers outsell Renault, Audi in August, report shows*, Reuters, 23 September 2025, https://www.reuters.com/business/autos-transportation/europes-plug-in-hybrid-boom-helps-chinese-carmakers-outsell-renault-audi-august-2025-09-23/
[4] V. Weber, M. Pericàs Riera, *Connected Vehicle Cybersecurity: The EU Must Consider Non-technical Risk Factors*, German Council on Foreign Relations, https://dgap.org/en/research/publications/connected-vehicle-cybersecurity-eu-must-consider-non-technical-risk-factors
[5] *Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats*, United States Department of Commerce, 14 January 2025, bis.gov.

China's Perspective: Strategic Opportunities Enabled by Connected Vehicles

In China, the automotive industry is at the heart of the state's technological strategy, positioned as a **driver of industrial upgrading** and **technological leadership.** Connected vehicles have been under Chinese authorities' attention since 2015, featuring in the flagship industrial strategy *Made in China 2025* as a key vector for the modernisation of China's automotive sector.[6] The expansion of intelligent transport systems is also a development priority in China's 14th Five-Year Plan for 2021–2025.[7]

As stated by the National Development and Reform Commission, Cyberspace Administration of China and a group of Chinese ministries: *"The **development of intelligent vehicles** helps enhance fundamental industrial capabilities, break through key technological bottlenecks, strengthen the **ability to lead a new round of scientific and technological revolution and industrial transformation,** and foster new competitive advantages for industrial development".*[8]

From China's perspective, connected vehicles are not confined to the civilian sector but are also intended to strengthen the military capabilities of the People's Liberation Army. This aligns with Xi Jinping's military-civil fusion policy (军民融合), which seeks to eliminate barriers between civilian research and the defense industry, with the ultimate goal of creating a world-class military. In this context, the **BeiDou satellite system is of particular importance to China.** On the one hand, the system provides precise navigation services for Chinese connected vehicles, while on the other it is **critical for military operations of the People's Liberation Army.**

As stated by the National Development and Reform Commission, the Cyberspace Administration of China, and a group of Chinese ministries: *"[Our main tasks include] … promoting the transformation and application of new technologies, including **carrying out joint military–civilian R&D efforts** and accelerating the application of the **BeiDou satellite navigation and positioning system** and high-resolution Earth*

[6] *"Made in China 2025" (中国制造2025),* State Council of the PRC, 19 May 2015, gov.cn; English-language version: *Notice of the State Council on the Publication of "Made in China 2025",* CSET, 10 March 2022, cset.georgetown.edu.

[7] *14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Objectives for 2035* (中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要), State Council of the PRC, 13 March 2021, gov.cn; English-language version: *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, CSET, 13 May 2021, cset.georgetown.edu.

[8] *Intelligent Vehicle Innovation Development Strategy* (智能汽车创新发展战略), National Development and Reform Commission, Cyberspace Administration of China, Ministry of Science and Technology of the PRC, Ministry of Industry and Information Technology of the PRC, Ministry of Public Security of the PRC, Ministry of Finance Ministry of Natural Resources of the PRC, Ministry of Housing and Urban–Rural Development of the PRC, Ministry of Transport of the PRC, Ministry of Commerce of the PRC, State Administration for Market Regulation of the PRC, 24 February 2020, ndrc.gov.cn. 24.02.2020, https://www.ndrc.gov.cn/xxgk/zcfb/tz/202002/t20200224_1221077.html

observation systems in ***intelligent-vehicle–related fields.”***[9]

As indicated by the Ministry of Industry and Information Technology: *“[China needs to]* ***support the construction of the BeiDou satellite navigation system*** *and facilities such as differential base stations, raise the level of the large-scale deployment of high-precision spatiotemporal services for vehicles, and* ***meet vehicles’ needs for high-precision positioning and navigation.”***[10]

[9] Ibid.

[10] *Action Plan for the Development Connected Vehicle Industry* (车联网（智能网联汽车）产业发展行动计划), Ministry of Industry and Information Technology of the PRC, 25.12.2018, https://www.gov.cn/zhengce/zhengceku/2018-12/31/content_5442947.htm.

China's Perspective: Security Risks Associated with Connected Vehicles

According to China's own assessment, connected cars collect extensive data and pose severe cyber security risks.[11] In Chinese state documents, the main risks to national security stemming from the growing number of connected cars are defined as follows: **1) connected vehicles increase the vulnerability to cyberattacks** (for example, the remote hijacking of cars or disrupting their sensors could lead to severe traffic accidents) and **2) connected vehicles collect sensitive data both from outside and inside the car** (e.g. data about critical infrastructure and the biometric data of the driver and passengers). Chinese regulators also pointed to the **risk of sensitive knowledge leaking abroad** through analyses of large datasets generated by millions of vehicles.[12] Such data could, for example, be used to map traffic patterns around military facilities, estimate levels of economic activity, or enable large-scale scanning and facial recognition of pedestrians.

In its domestic market, China adopts a highly cautious stance toward foreign manufacturers of connected vehicles. For example, until recently**, foreign connected vehicles operating in the Chinese market**—most notably Tesla, a US company manufacturing cars in Shanghai since 2019—were subject to **informal restrictions on driving or parking near government buildings, military facilities, airports, major highways, and locations hosting events involving senior Chinese Communist Party officials, including Xi Jinping.**[13] This was the case despite the fact that, as early as 2021, Tesla established a data centre in Shanghai to comply with requirements mandating the local storage of data generated in China.[14] In 2024, two Tesla models passed the security certification process, following a series of tests that verified the brand's compliance in four key areas: **(1) the anonymisation of facial and off-vehicle data, (2) the prevention of default cockpit data collection, (3) the in-vehicle processing of cockpit data,** and **(4) user notification on personal data processing.**[15] Formally, participation in data security tests is

[11] *Guidance on the "Technical Requirements for Vehicle Information Security of Intelligent and Connected Vehicles"* (智能网联汽车整车信息安全技术要求》解读), Industry and Information Technology Bureau of Shenzhen Municipality, 2023, sz.gov.cn

[12] *Basic requirements of security testing for sensing system of intelligent and connected vehicle spatio-temporal data* (智能网联汽车时空数据传感系统安全检测基本要求), Standardization Administration of China, 2023, std.samr.gov.cn.

[13] *Yueyang Airport has 'banned Teslas from entering,' but Changsha Airport and Changsha South Railway Station do not have similar rules* (岳阳机场"禁止特斯拉入内"，长沙机场、长沙南站没有类似规定), People's Government of Hengyang, 15 August 2023, hengyang.gov.cn; Z. Yan, Q. Li, B. Goh, *Tesla cars barred for 2 months in Beidaihe, site of China leadership meet*, Reuters, 20 June 2022, reuters.com; *Tesla cars barred from some China government compounds*, Reuters, 21 May 2021, reuters.com; *Tesla cars banned from China's military complexes on security concerns*, Reuters, 19 March 2021, reuters.com

[14] D. Yi, F. Murphy, *Tesla Announces New Shanghai Data Center to Allay Concerns*, 26 May 2021, caixinglobal.com

[15] *Notice on the Testing Results for Compliance with Four Security Requirements for Automotive Data Processing (First Batch)* (关于汽车数据处理4项安全要求检测情况的通报（第一批）, China Association of Automobile Manufacturers, 28 April 2024, caam.org.cn

voluntary and open to domestic and foreign manufacturers. However, in practice, it may serve as an **informal prerequisite for uninterrupted market access**. Only after obtaining data security certification did Tesla announce that this certification would enable its vehicles to gain broader access to the aforementioned locations.[16]

[16] D. Ren, *Elon Musk in China: Tesla passes data security assessment that could pave way for lifting of bars to its cars' movements*, South China Morning Post, 29 April 2024, scmp.com

China's Regulatory Approach: Embedding National Security into Connected Vehicles

In response to the technological revolution in the automotive sector, China has opted for strict control over connected vehicles. This approach is based on two core statutes: the Cybersecurity Law (2017) and the Data Security Law (2021).[17] Together, they impose a range of obligations on car manufacturers, including requirements to store key data exclusively within China—any cross-border transfer is subject to approval by the Cyberspace Administration of China; to implement security management systems; to classify data according to its importance, including its relevance to national security; and to conduct risk assessments and report their findings to regulators.

However, **Chinese authorities argue that the disruptive nature of connected vehicles necessitates the continual updating of regulatory frameworks.** Therefore, laws are progressively supplemented by administrative regulations and technical standards that can be updated rapidly as connected vehicle technologies evolve. The **Ministry of Industry and Information Technology** and the **Standardisation Administration of China** oversee the development of this framework. The National Technical Committee of Auto Standardization is under their remit, including its TC114/SC34 subcommittee on Intelligent and Connected Vehicles (全国汽车标准化技术委员会智能网联汽车分技术委员会编号TC114/SC34).18 In addition, practical enforcement of data security requirements is assessed through **data security certification schemes** administered by the **China Association of Automobile Manufacturers** (中国汽车工业协会) and the **National Computer Network Emergency Response Technical Coordination Center of China** (国家计算机网络应急技术处理协调中心).19 These two institutions subsequently **certified two Tesla models as meeting the four automotive data security requirements** under the scheme.

[17] *Cybersecurity Law of the People's Republic of China* (中华人民共和国网络安全法), Standing Committee of the National People's Congress, 7 November 2016, amended 28 October 2025, cac.gov.cn; English-language version: *Translation: Cybersecurity Law of the People's Republic of China*, 29 June 2018, digichina.stanford.edu; *Data Security Law of the People's Republic of China* (中华人民共和国数据安全法), Standing Committee of the National People's Congress, 10 June 2021,cac.gov.cn; English-language version: *Data Security Law of the People's Republic of China*, National People's Congress,9 December 2021, npc.gov.cn

Implications for Europe

To date, China has approached smart vehicles primarily from a defensive standpoint, building an extensive set of regulatory tools designed to shield the state from risks related to unauthorised data collection and vehicle cybersecurity vulnerabilities. However, **China may adopt a more offensive posture in the future**. This possibility is underscored by the country's highly developed offensive cyber capabilities, mature intelligence ecosystem, and signals contained in selected strategic documents, such as state guidance on integrating civilian and military technologies in the development of connected vehicles. China's domestic regulatory framework, combined with its own assessments of cybersecurity risks, clearly point to a **consistent perception of connected vehicles through a national security lens**.

This matters most acutely for **NATO's eastern flank**, given the deepening **China–Russia relationship** and the risk that data gathered by Chinese intelligent vehicles on European roads could ultimately be shared with the Russian Federation. Simultaneously, connected vehicles—regardless of the manufacturer's country of origin—are **vulnerable to cyberattacks** and the **exploitation of their sensors for intelligence purposes**, and, given their remote-control capabilities, also to acts of sabotage. Beyond considerations of cyber risks specific to the Chinese vector, **regulatory thinking on such vehicles across Europe should include the imposition of higher cybersecurity standards for all market participants.**

Connected vehicles are not currently comprehensively regulated at either the EU or national level. However, given the disruptive nature of this technology, an enforceable regulatory framework is required to prevent the automatic transfer of sensitive data abroad and mitigate the risk of cyberattacks.

Recommendations

Existing EU-level and national regulations lack detailed audits that would enable the systematic and practical verification of the cybersecurity and data protection safeguards applied to connected vehicles. Consequently, most member states currently lack the tools needed to assess, in a structured manner, the extent to which risks explicitly identified in Chinese policy and regulatory documents are materialising within the EU. Given the fundamental nature of the threats posed by connected vehicles, the introduction of such instruments is indispensable—not only from the perspective of cybersecurity and the protection of personal data, but also, more broadly, for the EU's digital sovereignty.

China's regulations on connected vehicles can serve as a useful starting point for understanding the risks associated with these technologies. To a certain extent, they can also be useful for designing a European regulatory environment to mitigate these issues. For example, Chinese regulators emphasise that intelligent vehicles can collect and transmit geospatial data relating to sensitive areas, such as critical infrastructure, potentially leading to the disclosure of state secrets.[18] Beyond risk classification, Chinese policy documents provide templates for certifying foreign manufacturers and verifying whether data are transmitted abroad.[19] They further point to specific technical solutions, such as a mode that disables off-vehicle data collection, which facilitates state authorities' ability to determine when a car is gathering data.[20] Therefore, Chinese solutions constitute a significant body of good practices. **Drawing on them would provide the EU with a strong argument when communicating any decision to introduce stricter regulations affecting connected vehicle from China to PRC authorities.**

What the EU could do next:

1) Member states must act immediately to **protect critical infrastructure** and **military facilities**, because the risk is already on our roads.

2) Intelligent vehicles should be firmly included in the **EU Cybersecurity Act revision**, because car-related risks are systemic and potentially greater than those associated with other Internet of Things objects.

[18] *Basic requirements of security testing for sensing system of intelligent and connected vehicle spatio-temporal data* (智能网联汽车时空数据传感系统安全检测基本要求), Standardization Administration of China, 2023, std.samr.gov.cn

[19] *Basic requirements of security testing for sensing system of intelligent and connected vehicle spatio-temporal data* (智能网联汽车时空数据传感系统安全检测基本要求), Standardization Administration of China, 2023, std.samr.gov.cn

[20] *Cybersecurity Standards: a Practical Guide. Guidance on "One-Click Stop" for Collecting Off-Vehicle Data* (网络安全标准实践指南–一键停止收集车外数据指引), National Technical Committee 260 on Cybersecurity of Standardization Administration of China, June 2024, tc260.org.cn.

3) **EU-side regulation** is needed as soon as possible; otherwise, **member states will regulate individually**, to the **detriment of the single market**, in a sector crucial for EU mobility. Done well, EU rules can be a potent non-tariff barrier and spur a booming, secure **EU-based car software and sensor industry.**

The EU should move swiftly to introduce bloc-wide rules obliging car manufacturers –particularly those from non-OECD countries, third countries, or non-allied states – to obtain additional data security certification. Such a mechanism would not only raise the level of safety across the internal market but could also facilitate the acquisition of technological know-how and encourage the localisation of higher value-added activities in Europe. In this way, the EU could push back against the increasingly pronounced trend of being reduced to a sales market or assembly base for Chinese products.

If establishing a common regulatory framework proves unattainable—whether due to resistance from some member states or prevailing deregulatory tendencies within the EU—**policymakers should proceed forming a coalition of countries committed to implementing additional data security certification.** This step should be buttressed by the development of a coherent set of harmonised standards at the EU level, for example, through a Commission-endorsed regulatory package that enables participating states to implement aligned rules. Such a mechanism would help mitigate the fragmentation of the single market while simultaneously raising security and technological resilience levels among the countries that choose to participate. In the absence of such an approach, the EU risks allowing regulatory inertia to harden into a structural vulnerability—undermining both the security of its internal market and its capacity to shape the technological rules that govern it.