# Chinese electric vehicles pose new national security risks in UK, warn experts



# The Growing Threat of Chinese Electric Vehicles in the UK: A Call for Vigilance

In an age where technology governs nearly every facet of our lives, the automotive industry stands at a critical juncture. Once viewed as mere modes of transport, modern vehicles have evolved into sophisticated computers on wheels, brimming with sensors and connectivity features. This transformation raises an alarming question: as China continues to expand its presence in the UK car market—now exceeding 10%—what implications does this have for national security?

Richard Dearlove, former head of MI6, has voiced grave concerns regarding the security risks posed by Chinese-manufactured electric vehicles (EVs). He suggested that these vehicles could easily be manipulated to disrupt traffic in London, underlining that this is a real threat rather than a mere scare story. With cars becoming increasingly reliant on internet connectivity, they are not just tools for transport; they can potentially serve as remote saboteurs in the hands of adversarial states.

The notion is not far-fetched when considering recent incidents. During an occupation in Ukraine, Russian forces commandeered advanced farming equipment; however, they soon discovered their inability to use these vehicles after being remotely disabled by the manufacturer, illustrating how connected technology can turn against its users. Similarly, serious concerns have arisen about the cybersecurity vulnerabilities inherent in electric vehicles. Demonstrations at cybersecurity conferences have shown how hackers have taken control of vehicle functions, raising alarms about the risks of espionage and targeted sabotage.

The Ministry of Defence has already begun taking precautionary measures, restricting the parking of EVs—especially those with Chinese components—near sensitive military establishments like RAF Wyton. This action reflects a broader anxiety within Western governments regarding critical infrastructure and foreign dependencies. However, these limitations could be just the beginning. As more Chinese EVs flood into the UK market, driven by government incentives in China and the rush for Net Zero targets, the potential for misuse rises.

Chinese firms are already making significant inroads into the market. Notably, brands such as BYD, Ora, and XPeng are gaining traction, supported by their competitive pricing—often influenced by government subsidies. Reports suggest that Chinese manufacturers could capture up to 25% of the UK market by 2030, as the government phases out the sale of petrol and diesel vehicles. This rapid expansion raises red flags among security experts and organisations alike, with warnings from figures like Professor Jim Saker of the Institute of the Motor Industry, who cautioned about the implications of Chinese technology serving as a “Trojan horse” for national security.

While concerns reach far beyond the automotive sector, they encapsulate a broader issue: the increasing reliance on Chinese technology in critical infrastructure. As articulated by UK MPs and security officials, the need for heightened vigilance against potential cyber threats has become paramount. There have been indications that household devices—be they electric vehicles, smart meters, or industrial machines—equipped with Chinese components could be exploited for espionage. Such vulnerabilities underscore the necessity for the UK to bolster its domestic production capabilities and reduce reliance on foreign tech, especially from nations with known adversarial agendas.

In a stark reminder of these risks, a tracking device originating from a Chinese component was reportedly found in then-Prime Minister Rishi Sunak’s car during a security sweep. While the government declined to confirm the specifics of the incident, it ignited further debates about hygiene and security protocols involving foreign-made vehicles. The inclusion of Chinese tech within both governmental and civilian infrastructures raises complex questions about sovereignty, privacy, and security.

In light of these concerns, there are calls to prohibit the use of Chinese-made vehicles within government fleets, with think tanks like the China Strategic Risks Institute advocating for a clear ban. The government’s commitment to eliminating petrol and diesel vehicles by 2027 complicates matters further, as Chinese manufacturers may see government contracts as an opportunity to grow while possibly compromising national security.

To navigate this precarious landscape, the UK must carefully consider not only its economic relationships but also the ramifications of allowing foreign technology into critical systems. As digital connectivity weaves into the fabric of our automotive future, securing that fabric against outside threats has never been more crucial. Moreover, in efforts to ensure national safety, both governmental and public sectors must remain agile, adaptable, and above all vigilant against the ever-evolving landscape of technological warfare.

The concerns surrounding Chinese EVs serve as a potent reminder of the intertwining relationship between technology, security, and national sovereignty. As policymakers grapple with these complexities, they must remain conscious that complacency could have far-reaching consequences for the UK’s future.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14688845/China-cripple-Britain-MI6-Beijing-IAN-WILLIAMS.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://www.thisismoney.co.uk/news/article-13910607/Chinas-share-UK-car-market-soars-10-FOLD-two-years-amid-fears-Beijing-electric-vehicles-weaponised-spy-Brits.html)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14688845/China-cripple-Britain-MI6-Beijing-IAN-WILLIAMS.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/0855641e-0eb2-4ee4-aada-8a322ba196bc)
* Paragraph 3 – [[2]](https://www.ft.com/content/0855641e-0eb2-4ee4-aada-8a322ba196bc), [[7]](https://www.telegraph.co.uk/business/2024/09/16/chinese-evs-in-britain-could-be-weaponised-think-tank-warns/)
* Paragraph 4 – [[3]](https://www.ft.com/content/518e6b5d-068a-4375-a625-87d8c5b422a1), [[5]](https://www.ft.com/content/822a6457-e543-4ab8-8457-1d7402f108c7)
* Paragraph 5 – [[4]](https://www.ft.com/content/534eef36-d9ad-4a03-afa1-f87ab03a9b18), [[6]](https://www.thisismoney.co.uk/news/article-13910607/Chinas-share-UK-car-market-soars-10-FOLD-two-years-amid-fears-Beijing-electric-vehicles-weaponised-spy-Brits.html)
* Paragraph 6 – [[1]](https://www.dailymail.co.uk/news/article-14688845/China-cripple-Britain-MI6-Beijing-IAN-WILLIAMS.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/0855641e-0eb2-4ee4-aada-8a322ba196bc), [[4]](https://www.ft.com/content/534eef36-d9ad-4a03-afa1-f87ab03a9b18)
* Paragraph 7 – [[3]](https://www.ft.com/content/518e6b5d-068a-4375-a625-87d8c5b422a1), [[6]](https://www.thisismoney.co.uk/news/article-13910607/Chinas-share-UK-car-market-soars-10-FOLD-two-years-amid-fears-Beijing-electric-vehicles-weaponised-spy-Brits.html)
* Paragraph 8 – [[1]](https://www.dailymail.co.uk/news/article-14688845/China-cripple-Britain-MI6-Beijing-IAN-WILLIAMS.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[7]](https://www.telegraph.co.uk/business/2024/09/16/chinese-evs-in-britain-could-be-weaponised-think-tank-warns/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14688845/China-cripple-Britain-MI6-Beijing-IAN-WILLIAMS.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/0855641e-0eb2-4ee4-aada-8a322ba196bc> - The UK Ministry of Defence is restricting electric vehicles (EVs) from accessing certain military bases due to concerns that Chinese-manufactured components in these cars could be used for espionage. RAF Wyton, home to intelligence operations, is one site where staff have been instructed to avoid parking EVs nearby. The Ministry emphasized that its security guidelines address threats from all vehicles, not just Chinese ones, and declined to provide a full list of affected sites for security reasons. This move aligns with broader Western apprehension about China's role in critical infrastructure, echoing prior decisions to exclude Huawei from UK telecom networks.
3. <https://www.ft.com/content/518e6b5d-068a-4375-a625-87d8c5b422a1> - UK MP Graeme Downie has warned that household devices containing Chinese electronics are at risk of remote sabotage, urging the UK to bolster its own manufacturing of cellular modules used in internet-connected devices. Downie highlighted potential threats posed by devices such as smart meters, electric cars, and drones, suggesting that China could exploit them for espionage or disruption. Downie's warnings come amidst broader government concerns over Chinese technology, with the UK already ordering the removal of Huawei components from its 5G network by 2027. The UK Ministry of Defence has also advised against conducting sensitive conversations in Chinese-made electric cars due to potential security risks. Downie, chair of the Coalition on Secure Technology, advocates for greater awareness and investment in UK technology to mitigate these risks. The government plans to introduce the Cyber Security and Resilience bill later this year to strengthen cyber defenses. China's Ministry of Foreign Affairs has dismissed these concerns as unfounded and accused the UK of politicizing economic and technological issues.
4. <https://www.ft.com/content/534eef36-d9ad-4a03-afa1-f87ab03a9b18> - MI5 is investigating the national security implications of Chinese technology in the UK's energy system, focusing on green technologies such as solar panels and industrial batteries. Concerns revolve around China's dominance in global supply chains crucial to decarbonisation and potential risks including data sharing with the Chinese government and control over strategic assets. The review is part of the UK's broader audit of its relations with China, set to report later this year. The discussion has extended to the Green Volt offshore wind project, where there is debate over the involvement of Chinese company Mingyang. MPs and experts worry about Chinese interference in critical infrastructure, sparking a debate on balancing pragmatic economic relationships with national security. The government has previously intervened to limit Chinese involvement in certain sectors, underscoring an inconsistent approach to Chinese participation in sensitive industries. The need to decarbonise Britain's power sector by 2030 presents a challenge, given the reliance on Chinese supply chains for renewables.
5. <https://www.ft.com/content/822a6457-e543-4ab8-8457-1d7402f108c7> - UK MPs are set to receive critical warnings concerning Chinese cyber attacks posing a threat to Britain's democracy, following the hacking of voter data and targeting of China hawks in parliament. Deputy Prime Minister Oliver Dowden will brief MPs and likely announce reprisals against individuals involved in these attacks, believed to be linked to Beijing. Security officials point to a complex cyber attack on the Electoral Commission, which occurred in August 2021. This warning comes amid concerns over increasing UK reliance on Chinese technology, highlighted by considerations from a Chinese firm to invest in a new UK gigafactory for electric vehicle batteries. MPs are expected to push for a tougher stance on China during these discussions. Downing Street and senior officials are focusing on the broader cyber threats from China facing the UK.
6. <https://www.thisismoney.co.uk/news/article-13910607/Chinas-share-UK-car-market-soars-10-FOLD-two-years-amid-fears-Beijing-electric-vehicles-weaponised-spy-Brits.html> - Chinese electric vehicles (EVs) are rapidly increasing their presence in the UK market, raising concerns about potential security risks. Experts warn that these vehicles could be used to spy on Britons, gathering information as they drive around the country and transmitting real-time intelligence back to Beijing. Professor Jim Saker, president of the Institute of the Motor Industry, highlighted the threat of connected vehicles flooding the country, potentially becoming an effective Trojan Horse for the Chinese establishment. The Institute of the Motor Industry has been collaborating with the National Protective Security Authority (NPSA) to address the security implications of state-of-the-art cars. Professor Saker emphasized that hackers could remotely disable the engine of a connected car, which has a constant internet connection to update software and provide location data, or unlock the vehicle remotely, making it easier to steal. He also noted that hackers could interfere with the car's operating features such as the horn, wipers, blinkers, or even headlights, leading to safety issues.
7. <https://www.telegraph.co.uk/business/2024/09/16/chinese-evs-in-britain-could-be-weaponised-think-tank-warns/> - Chinese electric vehicles (EVs) in Britain could be 'weaponised' and should be banned from government use, according to a report by the China Strategic Risks Institute (CSRI). The think tank warned that modules within Chinese-made EVs could transmit sensitive data back to China or even be remotely controlled. The report called for an end to Chinese carmakers being able to win government contracts. Last year, it emerged that the Ministry of Defence used electric cars made by Chinese-owned MG. The CSRI and the Coalition on Secure Technology, a group focused on risks from Chinese internet modules, are calling for a ban on EV and CIM manufacturers suspected of having ties to the Chinese government from being able to bid on public contracts.