CHINA STRATEGIC RISKS INSTITUTE

Collision Course: Under-pricing Chinese EV risks in the UK

Sam Goodman

September 2024

September 2024

About the China Strategic Risks Institute

The China Strategic Risks Institute (CSRI) is a non-profit, non-partisan research institute providing in-depth analysis of the risks and opportunities posed by the rise of the People's Republic of China. We aim for our research to be accessible to the general public, with recommendations for policymakers, international businesses and NGOs. The CSRI is not a political campaign or lobbying group.

www.csri.global

Acknowledgement

This report has been produced with the support of the Coalition on Secure Technology, a cross-party group of academics, industry experts and policymakers who are campaigning to raise awareness of the threat from Chinese-made Cellular IoT Modules.

www.cim-coalition.co.uk

CHINA STRATEGIC RISKS INSTITUTE

COALITION ON SECURE TECHNOLOGY

THE CELLULAR IOT MODULE THREAT

Table of Contents

Disclaimer

None of the companies or organisations discussed in this paper are accused of breaking any law, unless explicitly referenced via a third-party source. The inclusion of any such entities in this analysis is for illustrative, informational, or analytical purposes only, and does not imply any form of illegal conduct, wrongdoing, or unethical behaviour unless substantiated by external references. Where allegations or claims of illegal activity are mentioned, they are based solely on verifiable third-party reports or reliable sources, which will be clearly cited.

Executive Summary

The UK Government is currently stuck in a holding pattern. On the one hand, it appears unwilling to join its closest partners (the EU and the USA) in increasing tariffs on cheap Chinese electric vehicles. At the same time, it has failed to bring forward any alternative measures to protect jobs in the UK automotive industry.

At the heart of this indecision appears to be an under-pricing of the economic and security risks that growing dependency on Chinese EVs presents. The UK's domestic car industry is responsible for 198,000 British manufacturing jobs and contributes 2.5% of GDP to the UK economy.

Compared to the US and most European countries, the UK's EV targets are much higher and harder to reach. The UK is an outlier in its ambitious Zero Emission Vehicle quota system, which requires UK automakers to ensure 22% of car sales this year are EVs or face a £15,000 fine for each non-compliant vehicle sold. These targets have faced criticism from UK manufacturers as unworkable, and analysis by CSRI finds that on the current trajectory of EV sales, the 22% target for 2024 will be missed. Rather than driving the green transition, the UK's punitive targets will accelerate dependency on Chinese EV producers, which are heavily subsidised and can sell EVs more cheaply. In the case of BYD (the top EV producer in the People's Republic of China (PRC)), a study by the Kiel Institute for the World Economy found that the Chinese EV manufacturers received at least £2.9 billion in direct government subsidies from 2018-2022.

Excess manufacturing capacity in the PRC's economy and EV sector - potentially five to ten million cars - is likely to exacerbate the UK's dependence. The Rhodium Group's research shows that the PRC could have the capacity to export 560,000 EVs annually to Europe in 2025, and this could surge to as many as 1.7 million EVs in 2026. According to the Society of Motor Manufacturers and Traders (SMMT), Chinese-made EVs have rapidly gained ground in the last four years, with their market share in the UK jumping from 2% in 2019 to 33.4% of new EV registrations in the first half of 2023.

Given the rapid growth of Chinese-made EVs in the UK market, there is a risk that the UK could be seen as a dumping ground and a potential backdoor into the European market. This could impact the UK's current tariff-free access for UK EV exports to the European Single Market, becoming a thorn in the side of the new UK Government's attempts to build closer ties with Europe. This may also be an obstacle to any green technology trade deal between the UK and USA, which aims to give UK car manufacturers access to subsidies and tax reliefs under the US Inflation Reduction Act.

The presence of Chinese-owned "legacy brands", such as MG and Lotus, may dampen the efforts of the UK Government and industry to take action against Chinese EVs. Luxury car makers, who represent a small part of the UK car industry, are also lobbying the Government against tariffs for fear of reprisals from the PRC.

Aside from the threat to the UK's manufacturing industry, the UK public remains largely unaware of the dependency, disruption, and data security risks Chinese EVs pose via Chinese manufactured Cellular Internet of Things Modules (CIMs) within them.

- **Dependency Risk:** Chinese EV producers winning UK government procurement contracts and providing EVs to the police, the armed forces, government departments, and local authorities, will create dependency which could be exploited by the Chinese Communist Party (CCP) to pressure the UK Government to change its policies towards the PRC.
- **Disruption Risk:** If relations between the UK and the PRC were to deteriorate, CIMs in Chinese EVs could enable the PRC to disable vehicles and thus cause significant disruption to the UK Government, the police force, the military, and the UK's trade supply chain. Whilst the likelihood of the CCP disrupting the UK Government and society through sabotaging EVs is low in the current circumstances, responsible governments should plan for the worst and minimise national security risks in advance.
- **Data Security Risk:** EVs report geolocation and performance data in real-time. This would allow the PRC to plot the movement of government and defence vehicles. Geolocation detail is far greater than can be obtained from monitoring mobile phones. Put together with other information, this could yield useful intelligence. For example, by syncing a mobile phone with a car's audio system, manufacturers can gain access to personal data. If CIMs contained backdoors – such as those found in the products of Chinese technology companies Huawei and HikVision – the amount of data which could be extracted could be considerable.

Recommendations

Chinese EV producers have already outlined plans to create factories in Europe to circumvent any tariffs imposed on imports. With this in mind, imposing tariffs alone will not be an adequate policy solution to deal with these risks. That is why the UK Government should consider a policy mix of the key recommendations below.

Trade remedies

The Rhodium Group has warned that countries seeking to protect domestic EV production and level the playing field would need to raise tariffs on Chinese EVs to at least 50% if sales are able to be rendered unprofitable in European markets.

- The UK Government should formally launch its own anti-subsidies investigation into Chinese-made EVs and ensure that tariffs level the playing field and respond to unfair state subsidies. To avoid losing tariff-free access to EU markets for its EV exports, the UK should match EU tariffs on Chinese EVs.

Data security

EVs are essentially computers on wheels. However, the General Data Protection Regulation (GDPR) that governs privacy for computer services was not created with the geopolitical challenge of data extraction, exploitation, and appropriation from states considered to be "systemic rivals" in mind.

- The UK Government should legally require foreign EV companies from a country where the UK does not have a data standards equivalency agreement to store data on UK servers and to commit not to transfer the data overseas under any circumstances. EV companies from these countries operating in the UK should be legally required to share their source code with the UK Government and allow regular inspections of their data storage operations globally as evidence that they are not covertly transferring data to clouds or servers overseas annually.[1]
- UK intelligence services and the National Cyber Security Centre should be authorised to work with the Information Commissioner's Office and the Competition and Markets Authority to investigate whether EV companies are transferring data surreptitiously overseas.
- A failure to comply with this legal obligation or evidence by the Information Commissioner's Office that foreign EV operators are refusing to comply with the sharing of their source code or provision of evidence regarding the storage of data globally, should lead to an automatic ban for a particular EV operator from the UK market.

Such a measure should be described at a bare minimum as "reciprocity". Since October 2021, China has enforced similar stringent data requirements for non-Chinese technology companies operating in the country, which are required to share their source code and commit to keeping data within the country.

[1] It should be noted that TikTok in the USA has shared its source code with trusted US cloud provider Oracle as part of Project Texas and even offered to build in a "kill-switch" for US authorities to prevent a ban in the USA.
Anthropic and OpenAI have agreed to give the US AI Safety Institute (which sits under the US Department of Commerce) access to new AI models which will include sharing some of their source code.

CIMs

Significant gaps remain in the UK Government's knowledge regarding the extent to which Chinese manufacturers of CIMs dominate the UK EV market.

- As a first step, the UK Government should introduce a legal responsibility for EV producers and EV charging producers to disclose to the Government the suppliers of key CIM components in their vehicles and outline the potential sources of vulnerabilities pertaining to each CIM component.
- The UK Government should legally require EV producers operating in the UK market to use trusted CIM producers.
- Under the Procurement Act, the UK Government has the power to add companies to a debarment list. This new unit should be used to debar Chinese CIM manufacturers that are suspected of having ties with the PRC's military-industrial complex, as well as Chinese EV producers from public procurement contracts.
- The Procurement Act's debarment list should cover other CIM manufacturers directly, indirectly, or beneficially owned by PRC companies or individuals (there is evidence that some Chinese CIM manufacturers are setting up notionally American or other foreign companies, presumably to circumvent any future bans on Chinese manufactured CIMs).
- The UK Government should actively support trusted CIM manufacturing of CIMs and offer tax incentives for producers of CIMs to relocate CIM manufacturing to the UK.

EV sales targets

- Ministers should urgently meet with established European, American, Japanese, UK, and Indian automotive providers to discuss their concerns regarding the EV quota system and consider reviewing the financial penalties currently in place.
- The UK Government should investigate the viability of introducing a subsidy for trusted producers to manufacture EVs or a direct subsidy for UK consumers to buy EVs.

Working with partners

- Ministers should enter into talks with the USA and the EU to discuss mutual standards on data security and regulatory alignment when it comes to EVs.
- The UK Government should ensure coordinated action with the USA and EU when responding to the national security and economic risks EVs present, potentially through the UK cooperating with the EU-US Trade and Technology Council.
- Cooperation and coordination on EV and CIM policies should be a part of any UK-EU Security Partnership and any discussion of a UK-USA green technology deal.

Part One: Under-pricing the data security and CIMs risk

Chinese EVs and EV components, in particular, Cellular Internet of Things (IoT) Modules (CIMs), present democratic countries with three risks: **dependency, disruption, and data security**.

Cellular Internet of Things (IoT) Modules (CIMs), in particular, present key vulnerabilities that allow a car's functionalities to be changed or disrupted by its own manufacturer or other actors. CIMs enable various smart functions in modern vehicles, regardless of engine type, allowing a car to collect and analyse data in its surroundings. While CIMs have vulnerabilities that can be exploited by third parties, their continuous connection to their original manufacturers, as part of their normal functioning, gives their manufacturers continued control over the performance of the CIM, which may be weaponised.

Charlie Parton, a research fellow at the Council on Geostrategy and a China expert who has researched the CIM threat, describes them as wireless components embedded in larger devices or sub-units that work as gateways through which data flows in both directions.

For EVs, the concern is that the potential massive influx of made-in-China EVs, equipped heavily with made-in-China CIMs, will create a new area of dependency on the PRC, create vulnerabilities that can be exploited for disruption, and allow huge amounts of data to be collected for surveillance purposes. The introduction of automated driving will multiply these issues.

EVs are also **increasingly being integrated into 'smart cities'.** This drive to incorporate technology into local infrastructure, is aimed at increasing safety, unlocking productivity, and spurring economic growth.

Glasgow, Belfast, Birmingham, Bristol, Hull, Manchester, Milton Keynes, London and Peterborough are all embarking on projects related to the development of smart cities. For example, Glasgow, as part of its 'Future City Glasgow' programme, has launched the Glasgow Operations Centre that 'combines CCTV, traffic management, security systems, and police intelligence to support real-time responses to incidents across the city'.

This pales in comparison with the PRC, which boasts over 500 smart cities. In August 2018, as part of the so-called "Golden era of relations", UK Government ministers suggested that the UK and the PRC could share expertise and jointly develop smart cities.

EVs and related technology and infrastructure are integral to smart cities. Local authorities seek to use data collected from EVs to regulate smart traffic systems, street lighting, or to coordinate responses to traffic accidents.

This digital connectivity is made possible by the CIM embedded within an EV, which allows it to communicate with smart infrastructure. For example, when an EV gets live traffic information from smart traffic lights, looks up data on the nearest charging point, or receives a software update, it does so through the CIM embedded within it.

Dependency Risk

At the same time as setting a stringent EV quota for automotive producers, the UK Government has outlined ambitious targets for the acquisition of EVs for its own use, including for ministers, the police, and the armed forces.

As heavily state-subsidised Chinese EVs attain a significant portion of the EV market share in the UK, it is likely that they will begin to win government contracts and create a government dependency which could be exploited by the PRC.

As it stands, around 25% of the ministerial fleet of cars are already ultra-low emission vehicles, with a target for all central government cars and vans to be EVs by 2027. As with the Government's EV producer quota system it looks likely that the greatest beneficiary will be Chinese EV producers who can afford to underbid their competitors.

The Ministry of Defence confirmed in September 2023 that its department uses electric vehicles and hybrids produced by MG, which is owned by SAIC Motor. This is unsurprising on cost grounds given the dire state of public finances.

In the EV bus sector, the Chinese company BYD is already making significant inroads. At least 1800 electric buses (at around £100,000 cheaper per bus) have been delivered by BYD in the UK as cash strapped local authorities move to Chinese EV producers over domestic producers.

As with Hikvision cameras, local authorities are unaware of security risks or human rights concerns bound up in Chinese-made goods. Nor are they likely to be able to shoulder the financial burden to use alternative providers where procurement decisions go wrong without the direct support of the Government.

The PRC has a long track record of weaponising supply-chain dependencies to economically coerce partners. Between 2009 and 2020, the PRC increased restrictions on critical mineral exports nine times, more than any other supplier and in 2014 lost a case at the World Trade Organization for attempting to coerce Japan by cutting off its supply of critical minerals.

The danger of dependency on the PRC for EVs is that it gives the CCP the ability to ransom UK policy in other areas. Implicitly or explicitly, the threat is to withhold supplies of vehicles, spare parts, or software updates if future UK governments go against CCP interests in areas such as human rights, Taiwan, and trade disputes. That the UK Government and local authorities are already susceptible to CCP pressure is evidenced by the recent decision not to name the PRC as behind the hack of the Ministry of Defence or of Edinburgh Council to cancel a twinning agreement with the Taiwanese city of Kaohsiung.

Disruption Risk

What functions do different CIM components in cars perform and what vulnerabilities do they present?

Cellular Internet of Things Modules (CIMs) enable greater connectivity between a vehicle and its surroundings, as well as enhance a vehicle's capabilities. The vulnerabilities which they pose include:

1. Engine Control Units (ECUs)
ECUs are specialized computers that manage and control different functions in a vehicle. They process information from sensors, make decisions, and control various systems to ensure optimal performance, safety, and efficiency. They include:

a. ADAS/AD ECU
The Advanced Driver Assistance Systems (ADAS) or Autonomous Driving (AD) Electronic Control Unit (ECU) poses the highest security risk. This component is critical for vehicle control and safety features. If compromised, it could allow hackers to take over essential vehicle functions, potentially causing accidents or endangering passengers.

b. Gateway ECU
The gateway serves as a central hub for communication between various ECUs in the vehicle. A compromised gateway could allow attackers to intercept or manipulate data across multiple systems, potentially affecting numerous vehicle functions.

c. Vehicle Control Unit
This unit manages overall vehicle operations. If compromised, it could allow attackers to manipulate critical vehicle functions, posing a significant safety risk.

d. Infotainment ECU
Infotainment systems often have internet connectivity and complex software, making them a prime target for attackers. They can serve as an entry point to other vehicle systems and may contain sensitive user data. If connected, a user's smartphone may also be compromised through infotainment systems.

2. Telematics
Telematics systems, which handle vehicle-to-everything (V2X) communications, are highly vulnerable due to their constant connection to external networks. They could serve as an entry point for remote attacks, potentially compromising vehicle systems or stealing sensitive data.

Figure 1: Functions of different CIM components used in EVs and the vulnerabilities they present.

Interference with EVs

If relations between the UK and the PRC were to deteriorate, CIMs in Chinese EVs would enable the PRC to cause significant disruption to the UK Government, the police force, the military, the UK's trade supply chain and more.

Whilst the likelihood of the CCP disrupting the UK Government through EVs is currently slight, responsible governments should plan for the worst. Future hostilities are not out of the question, particularly with the PRC's militarisation of the South China Sea and military tensions within the Taiwan Strait. Moreover, the risk increases if central and local governments purchase Chinese EVs.

It is possible to shut down an EV or interfere with its functionality using real-time updates or instructions sent via the CIM. This is what John Deere did in May 2022 when it remotely shut down agricultural vehicles stolen by Russian soldiers in the occupied city of Melitopol. This could also be done by the suppliers of CIMs through firmware updates.

As Professor Jim Saker, President of the Institute of the Motor Industry, has warned, Chinese EVs could be used as a Trojan horse to disrupt the UK economy.

According to the Mayor of London traffic congestion costs the economy of London £5.1bn a year in lost productivity. If a CIM provider could shut down several EVs in an already congested area of London, it would create significant transport and economic disruption.

In a paper by New Kite Data Labs analysing the data functionality of EVs, Christopher Balding noted that it would be entirely possible to hack key components in an EV, including the braking system.

In 2022, David Colombo, a 19-year-old German hacker used a third-party application with access to Tesla's Application Programming Interface to get into the systems of more than two dozen Teslas around the world, controlling their locks, windows, and sound systems and downloading a huge bundle of information. Nor is David Colombo the first person to hack a car remotely. In 2015, two security experts in the US were able to remotely hack and drive a Jeep Cherokee and control its windshield wipers, its air-conditioning, and its brakes.

CIMs within Chinese EVs might be used to hack and disrupt the ministerial fleet. In 2020, the German Government accused Russia of hacking the military transportation authority which manages the ministerial fleet and travel logistics of its government departments.

According to the Cabinet Office, 'the military is the ultimate guarantor of national security and resilience in emergencies'. At least nine scenarios in the Government's National Risk Register

state the military is to respond to national emergencies ranging from a fuel crisis, flooding, and terrorism.

As the military and the police force transition to electric vehicles, their ability to respond to national emergencies could be disrupted if they use Chinese EV producers that have Chinese CIMs within them.

EV charging

US CIM provider Telit Cinterion outlines on their website the centrality of CIMs in allowing charging infrastructure and EVs to communicate and share data, giving the example of European drivers having one charging subscription account which would access charging infrastructure across the EU.

Ken Munro, a cofounder of UK company Pen Test Partners, has warned about the security risks of charging infrastructure being used to attack the grid. Spending 18 months analysing seven popular EV charger models in the UK and finding five had critical flaws, Ken said:

"It's not about your charger, it's about everyone's charger at the same time." Many home users leave their cars connected to chargers even if they aren't drawing power. They might, for example, plug in after work and schedule the vehicle to charge overnight when prices are lower. If a hacker were to switch thousands or millions of chargers on or off simultaneously, it could destabilise and even bring down grid systems."

The targeting of infrastructure has become an increasingly popular tactic of hostile states and hackers alike. In May 2024, US officials accused the PRC of conducting a sweeping cyber espionage campaign to hack US infrastructure organisations and map critical US infrastructure.

It is possible that using CIMs a hostile power might gather intelligence about the UK's energy grid with a view to a future attack on the system.

Data Security Risk

The software and hardware of EVs **collect a significant amount of data**, given the demands of autonomous driving, navigation, infotainment, and other safety and sensory diagnostics. Through the CIM vehicles receive software and firmware updates, connect to traffic grids, and receive travel updates.

Within the industry, there is no consensus on how much data a connected EV currently generates a day, but some estimates have put the upper limit at 32 terabytes of data per day. With the average iPhone having a storage capacity of 256 gigabytes, this would be the equivalent of an EV producing the data storage demand of 128 iPhones a day.

All this data is being continually transmitted to a cloud data centre accessible by the car manufacturer, so it is little surprise that the former head of MI6 has described an EV as a security risk and a "computer on wheels". This requires policymakers to think carefully about how to mitigate these risks.

EVs report geolocation and performance data in real time. This would allow a hostile state to plot the movement of all-or individual- government and defence vehicles. Put together with other information, this could yield useful intelligence. Additionally, by syncing a mobile phone with a car's audio system, manufacturers can gain access to personal data including access to the messages on someone's phone, their contacts, their files, or perhaps even their banking details.

If CIMs contain vulnerabilities or even backdoors – such as have been found in the products of Chinese technology companies Huawei and HikVision – the amount of data which could be extracted could be considerable.The leading Chinese manufacturer Quectel already advertises this service on its website as part of a 'vehicle tracking system' that offers 'real-time management of vehicle fleets via any computer or mobile phone'.

On 6 January 2023, inews reported that the geolocation data and movements of the Prime Minister's car believed to be a Land Rover was tracked by the PRC through a CIM.

Several media organisations have reported that Tesla cars in the PRC have been banned from driving near military sites and government buildings on national security grounds. A visit by Xi Jinping to Chengdu saw the authorities ban Tesla cars from the city.

After Tesla agreed to integrate Chinese technology company Baidu's navigation system into its cars in the PRC, it was announced in April 2024 that the US car brand had passed PRC data security tests. Clearly the PRC is aware of the risks CIMs within EVs present for spying. They are likely to exploit such vulnerabilities themselves.

A growing number of EVs integrate facial recognition software into their onboard cameras as a safety feature. However, the worry is that such data, which might come from a military site that is available to the manufacturer, could be sent back to the PRC.

This is more than a theoretical worry. In their internal messaging system from 2019-2022 Tesla employees shared videos taken from EVs through Sentry Mode (an intelligent vehicle security system) in the homes of private owners.

Legal requirements for EV producers and CIM producers to work with the PRC

The dominance of the PRC within the CIM supply chain creates a significant risk in most areas of critical national infrastructure but especially in EVs. It is not just the manufacturers of EVs, but also the manufacturers of CIM modules who gain access to customers' data.

In the PRC, the authorities have required access to EV data since 2017. Both domestic and foreign automakers must transfer mechanical and navigation data to local government-run data centres, where it is then pooled into a central platform managed by the Ministry of Industry and Information Technology and the Beijing Institute of Technology.

Under Article 36 of the PRC Data Security Law (2021), all data handlers (in this case, CIM manufacturers) are prohibited from providing any data stored in the PRC to foreign governments without approval from PRC authorities, regardless of the data's sensitivity level and where the data was originally collected.

Article 7 of the PRC's National Intelligence Law (2017) goes even further, stating that all PRC organisations and citizens have a responsibility to 'assist, support, and cooperate with national intelligence efforts' and that it is illegal to disclose the extent of that cooperation with a foreign government.

Thus, PRC CIM manufacturers not only have a legal obligation to collect data for the PRC's Ministry of State Security, but legally they cannot share the data they collect or disclose the extent of that collaboration with the UK or any other foreign government.

PRC domination of the CIM supply chain

As with previous policy debates in the UK regarding dependency on PRC companies in the UK's telecommunications network and surveillance infrastructure, the domination of PRC companies in the CIM supply chain is a question of ensuring the Government and the public uses "trusted vendors" who will not undermine national security and are not linked to gross human rights violations.

Alongside other parts of the EV supply chain, the PRC dominates the production of CIMs, with PRC companies having a market share of 63% globally in 2022 and 35% in Europe. Four out of five of the largest global producers of CIMs are based in the PRC.

Company	Headquarters	Global Market Share 2023 (Source: Counterpoint Research)

Quectel	PRC	34%
Fibocom	PRC	8%
China Mobile	PRC	7%
Telit Cinterion	US/France	7%
Sunsea	PRC	6%

Figure 2: The PRC dominates the production of CIMs and hosts four out of the five largest CIM producers globally.

The three leading PRC CIM Providers, Quectel, Fibocom, and China Mobile are all key suppliers of cellular IoT to PRC technology companies, which include HikVision, HiSilicon, DJI, and ZTE. All four of these companies are subject to export controls in the USA; HikVision is subject to US investment restrictions.

Both Quectel and Ficocom are intimately connected with these companies, sharing R&D, funding, staffing and ownership (one board member at HikVision is listed as a major shareholder at Quectel).

China Mobile, the other PRC market leader, was blacklisted by the US Government for its links to the People's Liberation Army and its involvement in civil-military fusion under the Trump Administration's Executive Order in November 2020 and the Biden Administration's Executive Order in June 2021.

The company also had its licence to operate in the USA revoked on national security grounds in 2019 and was de-listed from the New York Stock Exchange in January 2021.

In April 2024, it was reported that China Mobile was being investigated by HMRC over alleged underpaying of taxes spanning over a decade, with it estimated that the blacklisted CIM provider may owe up to £1.5m in unpaid tax.

These questionable partnerships and intimate involvement in civil-military fusion[2] in the PRC should be enough to disqualify PRC CIM providers from being considered "trusted providers" for EV producers within the G7.

[2] Civil-military fusion is a PRC strategy to eliminate barriers between China's civilian research and commercial sectors, and its military and defence industrial sectors.

PRC companies with links to the PLA or human rights violations involvement in the EV market

Unfortunately, the growing integration of technology in EVs or charging infrastructure from Chinese companies (who are not CIM providers) which are blacklisted or accused of having deep links with the People's Liberation Army or with gross human rights violations against Uyghur Muslims in Xinjiang adds ethical and additional security risks to the UK's growing dependency on Chinese EVs.

In the case of Zeekr, a Chinese EV company that boasts the integration of facial-recognition software to help owners unlock their EVs, in IPO documents to international investors it flagged directly the substantial influence the Chinese Government has exerted over its business.

BYD, one of the most competitive Chinese EV brands in Europe, has three research and development centres that are involved in military-civil fusion initiatives, with bi-directional exchanges between the military and the civilian/commercial sector.

Another cause for concern is the growing number of partnership agreements signed between foreign automotive companies and Chinese technology companies to help manufacture a viable EV product.

Japanese car manufacturer Honda Motors has partnered with Chinese facial recognition company SenseTime, which has been blacklisted by the USA for the provision of surveillance equipment targeting Uyghur Muslims in Xinjiang. Similarly, Japanese car manufacturer Toyota has formed a 'strategic alliance' with Chinese technology company Tencent, which had its ESG rating downgraded in 2023 for complicity in internet censorship in the PRC.

Chinese Technology Company	**EV involvement**	**Blacklisted/human rights record**
Huawei	EV car producer	On the US Entity list and banned in the USA. Some restrictions are required in participating in the following countries' telecommunications networks: the UK, Australia, New Zealand, Japan, Sweden, Romania, Estonia, Denmark, France, Latvia, Germany, Italy, Portugal, and Lithuania.
DJI Automotive (Zhuoyu)	CIM supplier	A subsidiary of DJI, which was sanctioned by the US for involvement in human rights abuses related

		to surveillance technology in Xinjiang and potential military ties.
Hesai Technologies	CIM supplier	Blacklisted for alleged ties to the Chinese military[3]
Quectel	CIM supplier	Under scrutiny and potential sanctions for alleged ties to the Chinese military.
Dahua Technology	EV charging infrastructure	On US blacklists for its role in the PRC's Military-Civil Fusion strategy. Banned in UK government departments.
Hikvision	EV smart bay parking solution	On US blacklists for its role in the PRC's Military-Civil Fusion strategy. Banned in UK government departments.
Alibaba	EV cloud storage	Allegations of complicity in human rights violations against Uyghur Muslims.
SenseTime	EV partnership with Honda Motors	On US entities investment blacklist.
Tencent	EV partnership with Toyota.	Allegations of complicity in human rights violations, including internet censorship.
Baidu	EV partnership with Tesla.	Allegations of complicity in human rights violations, including internet censorship.

Figure 3: Chinese technology companies with substantial involvement in EV production, their alleged records of human rights violations, and blacklisting by the USA and its allies.

[3] Hesai Technologies was blacklisted at the time of writing and is due to be removed from the entities list by the Department of Defence. See Financial Times 2024.

The Government's mixed response to data security

The UK Government's response to wider data security risks presented by PRC technology companies has been mixed. Getting key policy decisions wrong is expensive. Overturning the decision to allow Huawei to participate in 5G networks cost nearly £2bn to the taxpayer. Removing HikVision surveillance cameras from government departments on national security grounds only came about through pressures from Parliament. HikVision cameras are still in use across the public sector, with officials conceding that there are over a million HikVision cameras in use throughout the UK.

The Government needs to take more seriously the disruption, dependency, and data security risks which Chinese EVs present. It needs to be understood that within EVs the national security concern are Chinese-manufactured CIMs. Without a unified cross-government approach to this significant challenge, the UK will end up, by virtue of inaction, the most at risk country in Europe.

Continued inaction could lead to the absurd situation where Huawei is banned from the UK's 5G telecommunications network on national security grounds, but Huawei EVs drive down UK streets collecting data, including from phones synced to their audio systems. Meanwhile, Dahua Technology and HikVision cameras banned in Whitehall, could be installed by local councils in charging infrastructure and EV bay parking software; while Alibaba could be catering to our EV cloud storage needs.

Part Two: Under-pricing the economic risk

Building Demand - UK Government regulation on electric vehicles

The UK is heading towards an economy that will be decarbonised and increasingly digitally connected. At the heart of both of these transitions will be the widespread adoption of electric vehicles.

According to a study by the University of Nottingham Trent in 2020 widespread adoption of EVs in the UK could see the country reduce overall carbon emissions by nearly 12%. However, policymakers have given little thought to the growing dominance of the PRC in the EV market, the risks of dependence on the PRC for net-zero, and the wider data risks.

Given the Government's commitment to hit net zero by banning combustion engines by 2030 and through an EV quota system. It is clear that European, American, and Japanese carmakers that are already established in the UK automotive market will struggle to meet the Government's EV quotas unless they sell EVs at a loss, assuming that they decide to remain in the UK market in the long term.

Instead, the most likely beneficiary of the Government's targets will be Chinese EV manufacturers which are able to produce EVs at scale given their excess manufacturing capacity and are heavily subsidised so they can sell them at a lower price point. It appears that the UK Government has inadvertently created a heavy-handed quota system that favours Chinese EVs and, without further policy action, will hand them a significant share of the UK automotive market.

Government targets and demand

Under the UK Government's current targets, all vehicles in the UK will be fully zero-emission at the tailpipe by 2035, and from 2030 onwards, new vehicles sold in the UK will need to at least be plug-in or fully-hybrid vehicles as new internal combustion engine (ICE) car sales will be banned.

On 4 January 2024, the Government introduced new regulations under the Climate Change Act (2008) to mandate ambitious EV production targets for automakers operating within the UK as part of its plans to achieve net-zero emissions. Carmakers and vanmakers have to sell an increasing portion of their total sales volume as Zero Emission Vehicles (ZEVs), which includes

EVs and other non-ICE vehicles like hydrogen fuel cell electric vehicles, according to a schedule to be finalised by the Government.

Failure to meet this quota, which is 22% for 2024, will see automakers issued with a £15,000 fine for each non-compliant vehicle sold.

Those who do not meet this ZEV quota can buy green credits to avoid paying fines. However, the most likely EV producers that will have an excess of credits as they already meet the Government's EV quota will be Chinese EV producers, such as BYD.

Table 1. Annual targets for ZEV sales shares from 2024-2035 for cars

Year	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**
Target	22%	28%	33%	38%	52%	66%
Year	**2030**	**2031**	**2032**	**2033**	**2034**	**2035**
Target	80%	84%*	88%*	92%*	96%*	100%*

*Target will be set out in future legislation.

Figure 4: The UK Government sets annual targets for zero emission vehicle sales for automakers operating within the UK.

Under the Government's consultation, it is estimated that these targets would see at the low end at least 59% of all car and van sales in the UK in 2030 being EVs.

These new mandated EV production targets have already caused controversy amongst automakers operating in the UK. Carlos Tavares, the CEO of automaker Stellantis, which boasts 13% of their current UK car sales as EVs, has criticised the targets as a recipe for automakers to sell cars at a loss and potentially face bankruptcy.

Martin Sander, the head of Ford in Europe, has said that Ford intends to divert sales of ICE cars from the UK to other markets to avoid fines under the UK's EV quota, citing weak EV demand. The decision by Ford to cut the supply of automobiles to meet the EV quota could impact Ford's investment in the UK and the jobs that investment creates in the future.

This is in line with research by the Society of Motor Manufacturers and Traders (SMMT), which found that EVs accounted for just 13.1% of the new vehicle registrations in the UK in 2023. 2023 also marked the first year since 2018 in which EVs failed to improve their market share in total new car sales in the UK.

Low demand for EVs may be explained in part by the fact that unlike other European countries, the UK Government has not introduced direct consumer subsidies to purchase electric vehicles. Ministers instead currently offer tax incentives including an exemption from Vehicle Excise Duty and the London Congestion Charge until 2025 for EVs.

Another reason for low demand has been the failure of the Government to properly invest in charging infrastructure or to meet its own targets for building more EV charging stations.

Some motor experts believe that the Government has jumped the gun when it comes to its aggressive quota, as there is little incentive for consumers to buy EVs in 2024 given that in 2028 the introduction of solid-state batteries will allow drivers to travel up to 900 miles on one charge.

As of August 2024, the current trajectory of EV sales suggests EVs will account for around 19% of all new vehicle registrations in 2024. This shortfall would equate to missing the sales target by 60,000 EVs by the end of the year. Projecting the number of registered new cars in the UK alongside the Government's targets for EVs, the UK will need to sell more than 3 million EVs in 2035 alone.[4]

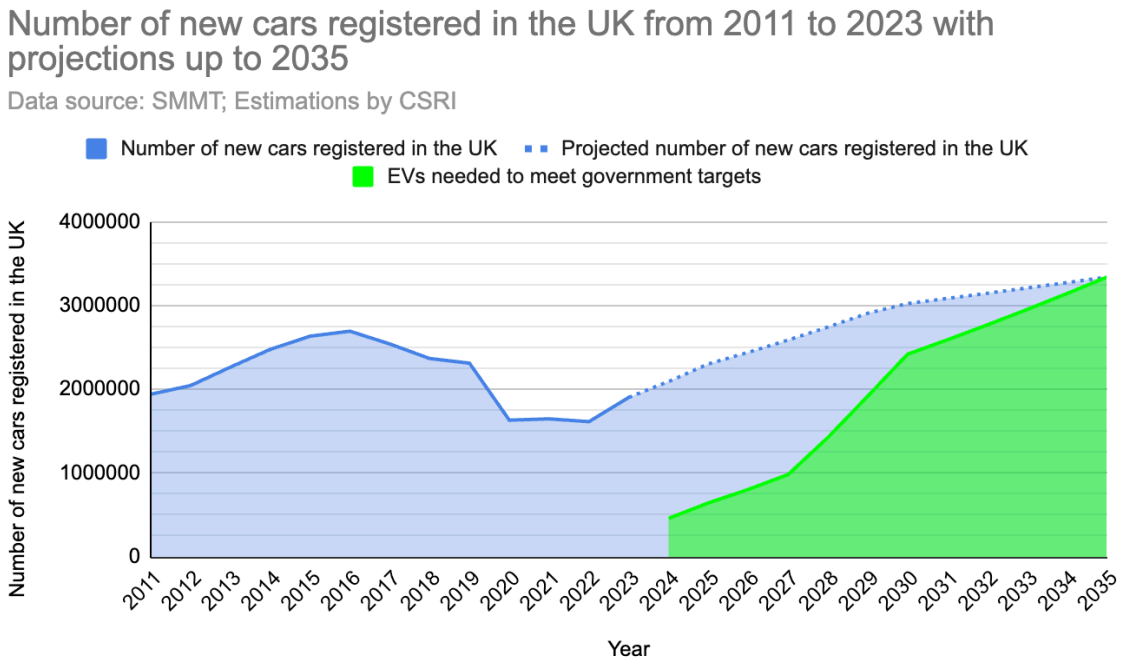

Figure 5: Number of new cars registered in the UK from 2011 to 2023 with projections up to 2035 (estimated by the CSRI).

[4]According to data from the SMMT, the UK sold a total of 1.9 million new cars in total in 2023. Assuming total car sales grow by 10% in the UK in 2024, a total of 2.1 million new cars will be sold in the UK in 2024. Assuming that new car sales grow annually by 10% in 2025, 6% from 2026-2029, 4% in 2030, and 2% afterwards, 3.34 million new cars will be sold in the UK in 2035. These assumptions are meant to bring the UK back to its 2015 pre-COVID peak in new car sales in 20226, with sales volume growth slowing down afterwards.

As mentioned above, the UK Government has inadvertently created a heavy-handed quota system that favours Chinese EVs and will, without further policy action, give them significant market share in the UK.

In the case of BYD, its Dolphin model is on sale in the UK at a starting price of £25,000, while the GWM Ora starts at £31,000. This is nearly less than half the average price for a European EV brand and significantly less than the average cost for an EV in the UK of £62,000. While the CEO of Chinese EV manufacturer Nio has stated that he believes Chinese EV manufacturers have at least a 20% cost advantage over their foreign competitors.

This appears to be the view of the Government, with the former Minister for Transport and Decarbonisation Anthony Browne stating at a Financial Times summit earlier this year that he did not expect carmakers to end up paying fines and that cheaper EVs from established brands and new Chinese brands would help build up demand.

Battery capacity

Another factor driving the import of Chinese EVs into the UK market is what an inquiry by the Business and Trade Committee in the House of Commons has described as the UK's 'gigafactory gap', i.e. the gap in domestic manufacturing capacity to meet companies' demand for EV batteries.

In a report published on 21 November 2023, the Business and Trade Committee warned that the UK is at risk of losing EV market share to cheap Chinese EV exports, and 160,000 jobs in the UK's automotive industry could be at risk if EV producers decide to "relocate operations overseas in countries hosting clusters of gigafactories".

Satisfying the battery demand from the automotive industry will require the UK to build up 100 gigawatt (GW) of battery manufacturing capacity by 2030 and 200 GW of capacity by 2040.

The British Government's response to the 'gigafactory gap' has been to accept investment from Chinese battery manufacturer Envision AESC for a 25-GW battery factory in Sunderland and Chinese battery manufacturer EVE Energy for an initial 20-GW battery factory in Coventry. Both of these gigafactories are expected to be completed and online by 2025.

Figure 6: New battery factories under construction or plan in the UK. Map created using Mapcreator.io.

The dominance of the PRC

The PRC policies to raise GDP growth continue to put weight on exports. Electric vehicles, lithium-ion batteries, and solar photovoltaic cells are important elements of that. According to Chinese Government officials, green exports rose by 30% to $147bn last year.

Under Xi Jinping's 'Made in China 2025' strategy, EVs are one of ten strategic industries in which China seeks global leadership by 2049. This includes a target of 80% of EVs being made in the PRC by 2025.

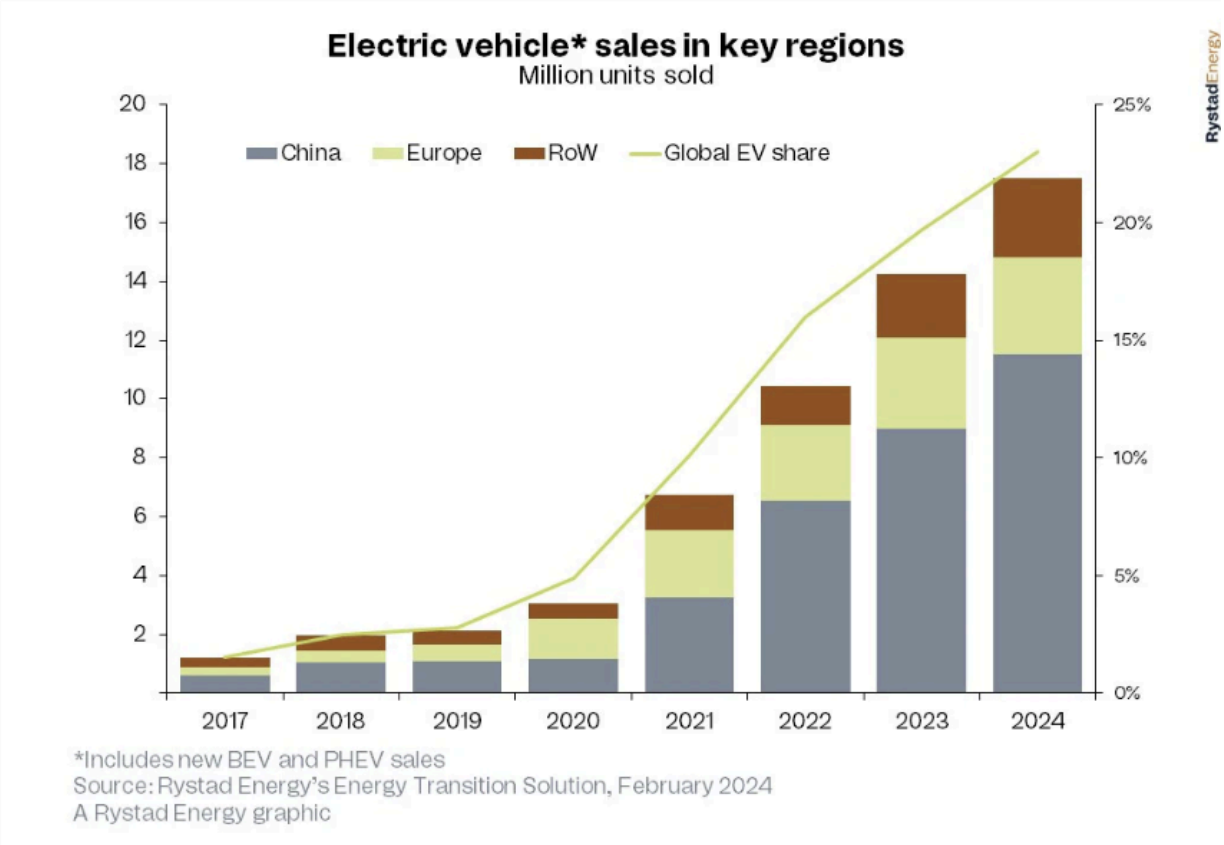

Figure 7: Annual growth of global EV sale shares in key regions, 2017-2024. Source: RystadEnergy, 2024.

This dominance has been built upon significant state subsidies. According to a study by the Kiel Institute for the World Economy, Chinese EV manufacturer BYD received at least £2.9 billion in direct government subsidies from 2018-2022 as part of the PRC's push to dominate electric vehicles and clean technologies. The subsidies to BYD jumped from around £195 million in 2020 to £1.8 billion in 2022 alone.

The PRC boasts the largest EV domestic market in the world, and it is also the largest manufacturer and exporter of EVs as well. In 2023, the PRC produced 9.3 million EVs and exported around 900,000 EVs to the rest of the world.

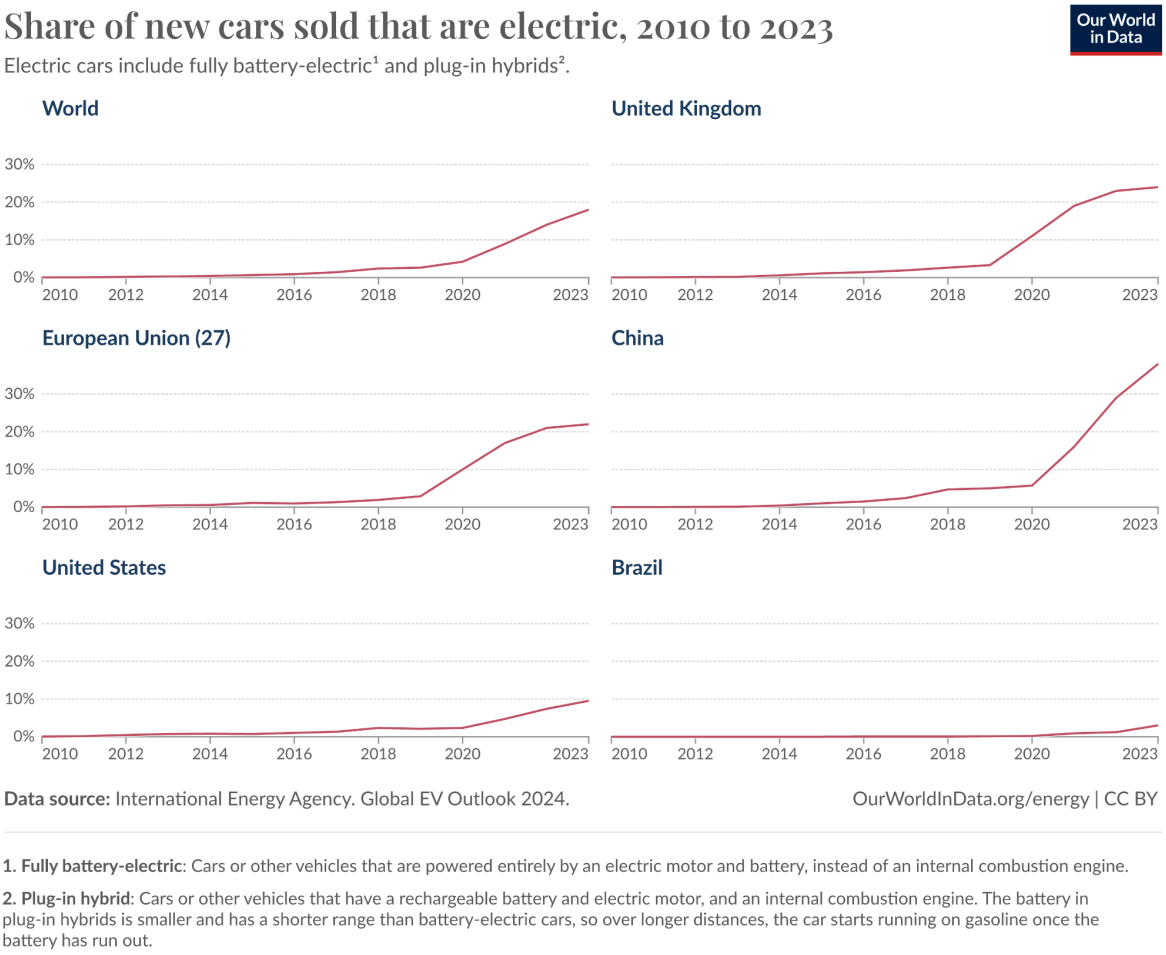

Figure 8: Shares of new cars sold that are electric, 2010-2023. Source: Our World in Data, 2024.

In the same year (2023), the PRC became the world's biggest exporter of cars, surpassing Japan. According to the PRC's General Administration of Customs, the PRC exported 3.2 million vehicles in 2022, compared to Germany's 2.6 million vehicle exports.

The PRC's EV market penetration in Europe, while relatively small compared to overall automotive sales, has grown rapidly from 1% in 2019 to around 8% in 2023. The European Commission has warned that this number could rise to 15% by 2025.

This is in line with the view of analysts who have assessed that excess capacity in Chinese automotive factories could be between five and ten million cars a year. The Biden Administration argues that the fact that the PRC's export of EVs has increased by 70% from 2022 to 2023 reflects excess manufacturing capacity.

The PRC's EV exports and ability to gain market share in the UK and Europe have been hindered by the scarcity of affordable shipping vessels and increased costs as a result of disruption in

the Red Sea. However, Chinese EV producers and shipping companies have moved to rectify this issue by placing orders for new ships.

According to research by the Rhodium Group, the PRC could have the capacity to export 560,000 cars annually to Europe in 2025, based on six trips a year (in 2023, the EU imported 472,000 EVs from the PRC), and capacity could surge to as much as 1.7 million cars in 2026.

Chinese industry dominates EV production from the upstream to the downstream: the extraction and refinement of critical minerals, the production of batteries and other components of EVs, and the assembly of EVs.

EV Sector/Supply Chain	**PRC Dominance**
Critical minerals refinement	The PRC refines 68% of nickel, 40% of copper, 59% of lithium, and 73% of cobalt.
EV battery production	Over 75% of lithium batteries used in EVs are produced in China.
EV production and exports	China exported 900,000 EVs in 2023 and made 9.3m EVs domestically.
Global production of Cellular Internet of Things Module (CIMs)	PRC companies have a global market share of well over 60%. Four out of five of the largest global producers of CIMs are based in China.
Excess manufacturing EV capacity for export to Europe	China could have the capacity to export 560,000 cars annually to Europe in 2025, and it could surge to as many as 1.7 million cars in 2026.

Figure 9: PRC dominance in each phase of the global EV supply chain.

Chinese EV sales in the UK

The UK's proximity to the EU and the Government's ambitious quotas for EV sales make the UK an attractive market for Chinese EV exports.

According to the Society of Motor Manufacturers and Traders (SMMT), Chinese-made EVs have rapidly gained ground in the last four years, with their market share in the UK jumping from 2% in 2019 to 33.4% in the first half of 2023.

This figure includes all Tesla models being made and imported from Chinese factories and reflects a dramatic drop in US cars imported into the UK at the same time.

At the same time, the UK's share of car exports to the PRC slipped to 7.4% in the first half of 2023, contributing to the UK's significant trade deficit with the PRC.

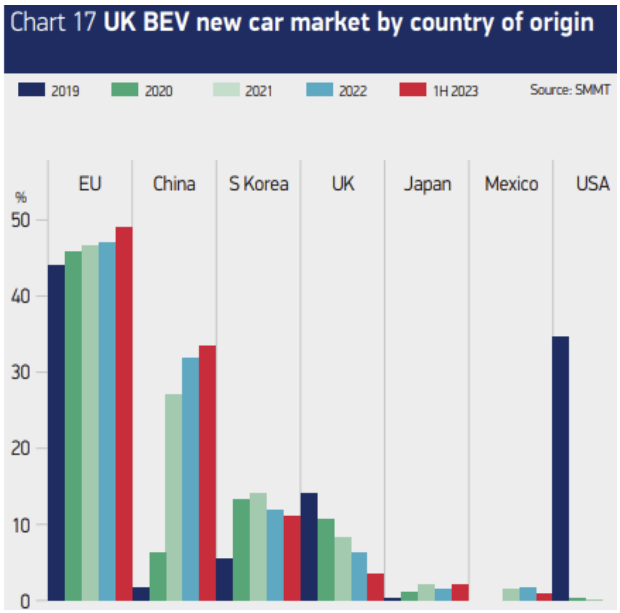

Figure 10: New BEVs sold in the UK market by country of origin, 2019-2023 (first half). Source: The Society of Motor Manufacturers and Traders, 2023.

Given these figures only account for the first half of 2023, it is likely that the overall percentage of Chinese EV imports into the UK will be at a lower rate when we account for the whole year. Reflecting on the rapid growth of Chinese-made EVs in the UK market in a few short years, it is not unreasonable to imagine that we could see Chinese-made EVs capture at least a third of the UK market share by the second half of the decade.

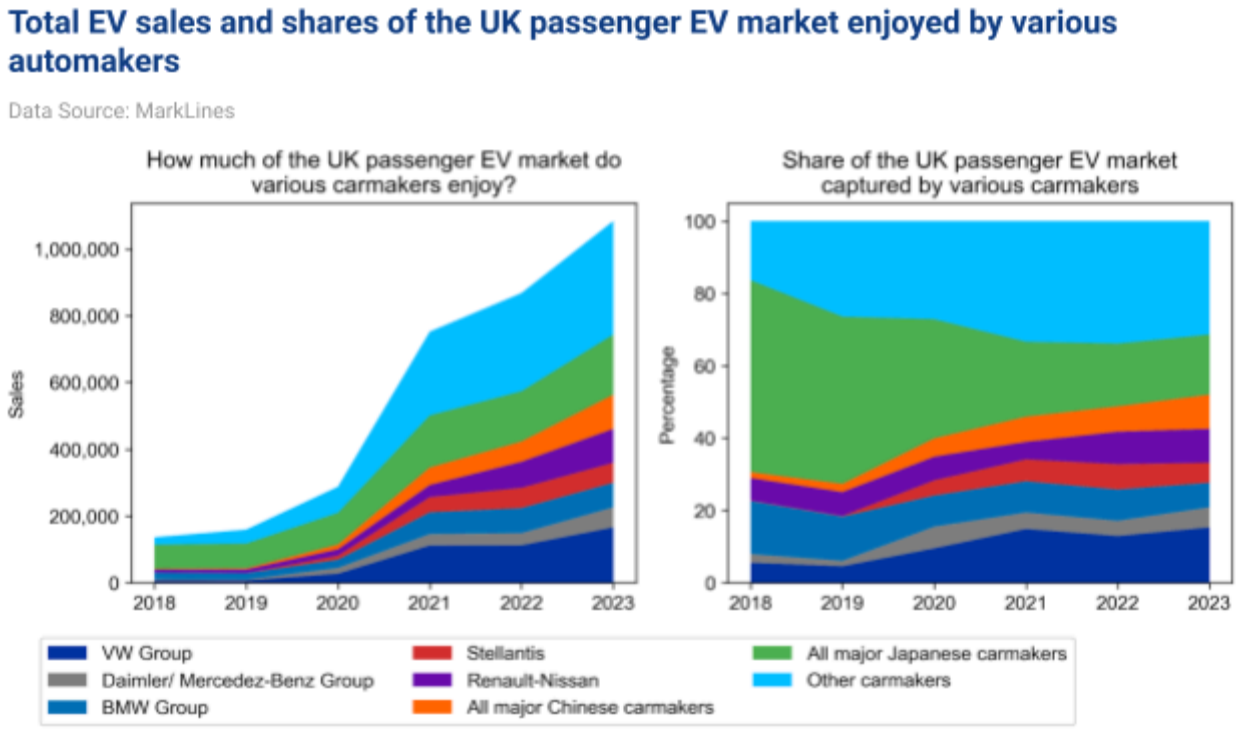

Figure 11: Total EV sales and shares of the UK passenger EV market enjoyed by various automakers. Data Source: MarkLines, 2024.

A lack of national champions

Unlike Europe, the UK has historic car brands, but it no longer has UK-owned national champions, having sold them off to foreign manufacturers throughout the 1990s, 2000s, and 2010s. Many of these brands ended up in the hands of historic US and European automotive companies.

For a time, this arrangement led to the best of both worlds: the UK car industry received much-needed foreign investment, and the UK boasted of hosting the largest number of foreign car manufacturers in Europe.

Despite a lack of national champions, the UK car industry employs 780,000 people across Britain, with 182,000 working directly in manufacturing. It accounts for 10% of UK exports, contributes £14 in value added for the UK economy, and invests around £3bn in research and development in the UK each year.

The foreign ownership model that has kept the UK car industry afloat is now facing converging pressure due to the trade barriers erected after the UK's exit from the EU. Rising European and American protectionist measures in response to the economic security challenges presented by the PRC adds to that pressure.

With a lack of national champions, the UK is more exposed to the economic threat posed by Chinese EVs than Europe. If foreign car manufacturers have to close factories in response to PRC competition, they will likely sacrifice UK factories rather than those in their home countries, particularly if the UK already has a "gigafactory gap" which will limit their future development.

UK car brand	Previous owner	Current owner	Year it was sold
Rolls-Royce Motor Cars	Rolls-Royce plc	BMW	2003
Bentley	Vickers	Volkswagen	1998
Jaguar	Ford	Tata Motors	2008
Land Rover	Ford	Tata Motors	2008
Mini	Rover Group	BMW	1994
Lotus	Proton	Geely (51%), Etika (49%)	2017
MG	MG	Nanjing Automobile Group	2006
Vauxhall/Opel	GM	PSA (-2017); Stellantis (2021-)	2017

Figure 12: UK car brands that were sold to foreign automobile groups.

PRC ownership of UK brands

This is further complicated by the sale of historic car brands to Chinese automakers throughout the so-called "Era of Golden Relations" between the UK and the PRC. In the case of Lotus, Chinese manufacturer Geely acquired a majority stake in June 2017.

Geely, like many Chinese automakers, has benefited significantly from PRC state subsidies. One study found that state subsidies in 2011 reached the equivalent of 51.3% of its net profits. While

in September 2019, it was reported the Hangzhou municipal government included Geely in a programme that would see government officials placed in the management structure of the automotive company.

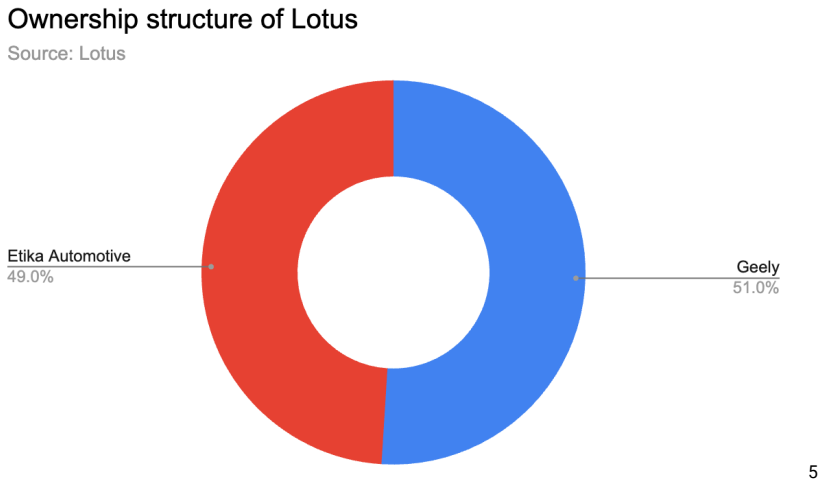

Figure 13: Chinese manufacturer Geely acquired a 51% stake in UK car brand Lotus in June 2017.

MG, one of the more popular EV car brands in the UK, was first sold to the Nanjing Automobile Corporation in 2005, from which SAIC Motor then acquired the brand in December 2007.[6] SAIC was advised by Rothschilds on the purchase of MG and the Secretary of State for Trade and Industry and the Prime Minister at the time personally negotiated with the Chinese Government to help broker the sale.

In comparison, in 2009, the German Government blocked the sale of Opel, the German car manufacturer owned by General Motors, to Beijing Automotive Industry Holding Co. on intellectual property and job security grounds.

Attempts in 2017 by the PRC's leading SUV maker, Great Wall Motor Co, to buy the Jeep brand from Fiat Chrysler were similarly scrapped after reports that the acquisition would not pass scrutiny from the Committee on Foreign Investment in the United States (CFIUS).

Few UK consumers and policymakers seem aware that SAIC Motor is majority-owned by and directly reports to the Shanghai municipal government through its State-owned Assets Supervision and Administration Commission (SASAC).

---

[5] Etika Automotive is a Malaysian conglomerate

[6] SAIC stands for "Shanghai Automotive Industry Corporation", but the company is now officially known as "SAIC Motor"

In effect, this means that the Shanghai Chinese Communist Party has the final say over the management direction of MG, one of the most popular automotive brands in the UK.

This does not seem to concern the Ministry of Defence, which in September 2023 confirmed that part of its EV fleet had been purchased from MG.

The SASAC's of the Central Government and Nanjing own smaller shares in SAIC, as do the state sovereign wealth fund China Investment Corporation (CIC) and the state-owned financial institution China Securities Finance Corporation (CSF).

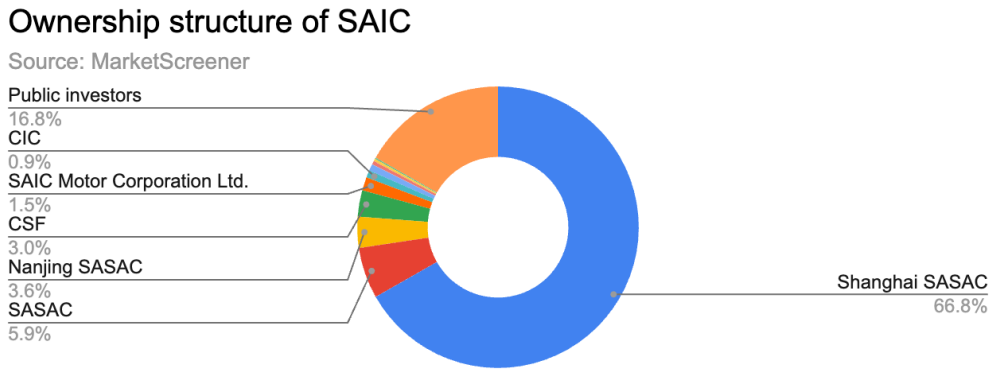

Figure 14: Chinese automaker SAIC is majority-owned by the State-owned Assets Supervision and Administration Commission (SASAC) (66.8%).

As with the solar industry trade associations in Europe, the presence of Chinese-owned companies within UK automotive associations could dampen calls from the sector for the Government to protect European automotive jobs from the economic and security risk presented by Chinese EV imports.

Tariffs to protect economic security: response from other countries to PRC EV exports

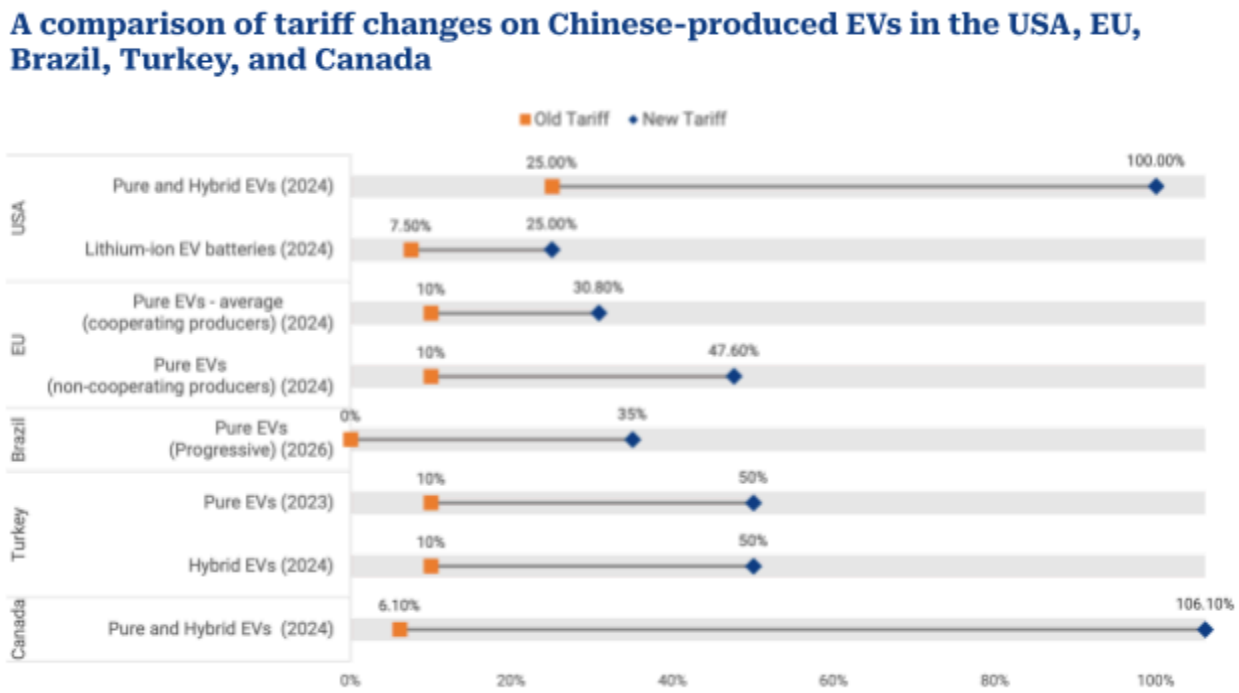

Figure 15: A global comparison of recent tariff changes on Chinese-produced EVs (respectively, the USA, EU, Brazil, Turkey, and Canada).

EU

In response to the surge of EV imports from the PRC, the European Commission announced on 5 July 2024 the conclusion of an anti-subsidies investigation and provisional countervailing duties on Chinese EVs ranging from 17.4% (for BYD) to 37.6% (for SAIC). Other producers are subjected to a weighted average duty of 20.8% depending on their level of cooperation with the investigation and the amount of subsidy received by the manufacturer. The tariff increase at the time of writing still needs to be ratified by the EU Council, with some EU Member States actively lobbying against them.

USA

Under the Biden Administration's Inflation Reduction Act (2022), Chinese EVs or EVs with a certain level of components from the PRC are considered to be a "Foreign Entity of Concern" and are not able to access tax credits under the scheme. On 14 May 2024, the Biden Administration announced that it would increase tariffs on Chinese EVs from 25% to 100% and on Chinese lithium ion-EV batteries from 7.5% to 25% in 2024.

Canada

Following a public consultation, the Canadian Government announced a 100% tariff on Chinese EV imports from 1 October 2024. Ministers at the same time announced a 25% tariff on Chinese steel and aluminium imports and a further consultation on future tariffs on solar, battery, semiconductors, and critical mineral imports from the PRC.

Brazil

Brazil has welcomed Chinese EV exports which accounted for 40% of all imports of EVs from January-March 2024. However, Brazilian President Luiz Inacio Lula da Silva has introduced a 10% tariff on EV imports, which rises to 18% in July 2024, and 35% in 2026, as a means of encouraging EV development in the domestic auto-industry.

Recommendations for policymakers

Chinese EV producers have already outlined plans to create factories in Europe to work around any tariffs imposed on imports. BYD has signed an agreement to open a factory in Hungary and the CEO of Chinese EV producer Nio has stated they will look for a manufacturing facility in Europe with a baseline of producing 100,000 units a year.

With this in mind, imposing tariffs alone will not be an adequate policy solution to deal with the risks presented by Chinese EVs, particularly those related to data security. That is why the UK Government should consider a policy mix of the recommendations below.

Trade remedies

The Rhodium Group has warned that countries seeking to protect domestic production of EVs and level the playing field would need to raise tariffs on Chinese EVs to at least 50% before sales become unprofitable in European markets.

- The UK Government should formally launch its own anti-subsidies investigation into Chinese-made EVs, ensure that tariffs level the playing field, and respond to unfair state subsidies. To avoid losing tariff-free access to EU markets for its EV exports, the UK should match EU tariffs on Chinese EVs.
- The risks of disruption, dependency, and data extraction apply to charging units just as they do to the EVs themselves. Ministers should consider extending powers to give a "designated vendor direction" to EV charging companies, which would require them not to use Chinese EV charging units in the UK's charging network.[7]

Data security

EVs are essentially computers on wheels. The General Data Protection Regulation (GDPR) was not created with the geopolitical challenge of data extraction, exploitation, and appropriation from states considered to be "systemic rivals" in mind.

- The UK Government should legally require foreign EV companies from a country where the UK does not have a data standards equivalency agreement to store data on UK

[7] These powers were used by Ministers to issue a "designation notice" against Huawei requiring UK telecommunications providers to ban Huawei equipment from the UK's 5G network.

servers and to commit not to transfer the data overseas under any circumstances. EV companies from these countries operating in the UK should be legally required to share their source code with the UK Government and allow regular inspections of their data storage operations globally as evidence that they are not covertly transferring data to clouds or servers overseas annually.[8]

- UK intelligence services and the National Cyber Security Centre should be authorised to work with the Information Commissioner's Office and the Competition and Markets Authority to investigate whether EV companies are transferring data surreptitiously overseas.
- A failure to comply with this legal obligation or evidence by the Information Commissioner's Office that foreign EV operators are refusing to comply with the sharing of their source code or provision of evidence regarding the storage of data globally, should lead to an automatic ban for a particular EV operator from the UK market.

Such a measure should be described at a bare minimum as "reciprocity", since October 2021 the PRC has enforced similar stringent data requirements for non-Chinese technology companies operating in the country who are required to share their source code and commit to keeping data within the country.

CIMs

Significant gaps remain in the UK Government's knowledge regarding the extent to which Chinese manufacturers of CIMs dominate the UK EV market.

- Ministers should undertake an audit of the security risks posed by CIMs within EVs, particularly any security vulnerabilities they pose.
- As a first step, the UK Government should introduce a legal responsibility for EV producers and EV charging producers to disclose to the Government the suppliers of key CIM components in their vehicles and outline the potential sources of vulnerabilities pertaining to each CIM component.
- The UK Government should legally require EV producers operating in the UK to use trusted CIM producers, which are assessed by regulators as not posing a data security risk.
- Under the Procurement Act, the UK Government has the power to add companies to a debarment list. This new unit should be used to debar Chinese CIM manufacturers Quectel, Fibocom, and China Mobile, as well as Chinese EV producers from public procurement contracts.

[8] It should be noted that TikTok in the USA has shared its source code with trusted US cloud provider Oracle as part of Project Texas and even offered to build in a "kill-switch" for US authorities to prevent a ban in the USA.
Anthropic and OpenAI have agreed to give the US AI Safety Institute (which sits under the US Department of Commerce) access to new AI models which will include sharing some of their source code.

- The Procurement Act's debarment list should cover other CIM manufacturers ultimately owned by PRC companies or individuals (companies such as Quectel are already setting up subsidiaries which are notionally Malaysian or American companies)
- The UK Government should actively support the manufacturing of CIMs and offer tax incentives for trusted CIM producers to locate CIM manufacturing in the UK.

EV sales targets

The UK is currently inadvertently turbocharging the market share of Chinese EVs with a stringent quota system that threatens financial penalties for established automotive providers.

- Ministers should urgently meet with established European, American, Japanese, UK, and Indian automotive providers to discuss their concerns regarding the EV quota system and consider reviewing the financial penalties currently in place.
- The UK Government should investigate the viability of introducing a subsidy for trusted producers to manufacture EVs or a direct subsidy for UK consumers to buy EVs.

Working with partners

Given that the USA and the EU have both embarked on their own separate subsidy schemes for the EV sector and taken measures to respond to the PRC's excess capacity and the risk of Chinese EV imports, the UK should look to work more closely with the USA and EU on this issue.

- Ministers should undertake and publish a risk analysis of the UK automotive industry's exposure to any economic downturn in the European automotive sector as a result of the import of Chinese EVs.
- Ministers should enter into talks with the USA and the EU regarding mutual standards and regulatory alignment when it comes to EVs.
- The UK Government should ensure coordinated action with the USA and EU in responding to the national security and economic risks EVs present, potentially through the UK joining the EU-US Trade and Technology Council.
- Cooperation and coordination on EV and CIM policies should be a part of any UK-EU Security Partnership.
- Cooperation and coordination on EV and CIM policies should be a part of any discussion regarding a UK-USA green technology trade deal, which would allow access to the USA Inflation Reduction Act.
- The UK Government should push for a Five-Eyes investigation into the data risks Chinese EVs present, with a particular focus on the use of CIMs to extract data to the PRC. This could form the basis of the development of a wider Five-Eyes data security protocol for EVs.