COMMENTARY
NO. 5 2024

SWEDISH NATIONAL CHINA CENTRE

Security concerns regarding Chinese connected cars: A short overview

The rise of electric vehicles (EVs) and smart car technology is raising increasing concerns about cybersecurity and data privacy. Large-scale data collection, hacking vulnerabilities and the possibility that malicious actors might be able to take control of privately owned vehicles are security concerns that all connected cars have in common. Deteriorating relations between China and the West, and especially the increased geopolitical rivalry between China and the United States, mean that Chinese manufacturers have come under particular scrutiny and the problem has acquired a national security dimension.

Security vulnerabilities of connected cars

Because of their high degree of connectivity, modern cars present a number of cybersecurity risks, most notably concerning data collection, hacking vulnerabilities and manufacturers' ultimate control over the vehicles sold.

First, a large number of features in a modern vehicle typically interface with the internet. The car's software is updated wirelessly and its functionality can be altered using functions that can be enabled or disabled through the internet. Cars also collect large amounts of data and transmit this to the manufacturer. According to one estimate, a typical modern car can generate 1400 gigabytes of data per hour, although most of this is deleted quickly and only a small fraction is sent to the manufacturer. Many cars collect data automatically, even from systems that are not being actively used. This has been shown to be the case for certain Chinese EVs. The type of data collected can include user profiles, including biometric information, and geographic data. Driving behaviour—such as acceleration, speed and steering patterns—can be recorded alongside more personal information such as voice commands and data from synced smartphones. This data can then be shared with various entities in addition to the manufacturer, such as affiliates, insurance companies and even government agencies.

In addition, connected cars are susceptible to hacking. If exploited, weaknesses in vehicle cybersecurity could allow malicious actors to control crucial vehicle functions remotely. In some models, nearly all functionalities could theoretically be operated wirelessly, including acceleration, braking and steering. If a hacker were to find a vulnerability in the software, the consequences could be catastrophic.

A final concern is that by design, the manufacturer retains a high degree of ultimate control over connected vehicles. A real-world example of this was demonstrated when Russia looted Ukrainian agricultural machinery in the early stages of the Ukraine war and the manufacturer, John Deere, stepped in to remotely disable the equipment.

Risks with Chinese manufacturers and components

In principle, these three vulnerabilities exist in all connected vehicles. The problem of highly connected electrical vehicles acquires a national security dimension, however, when there is exposure to countries that are considered high risk. Today, many countries, including in Europe, identify China as a security concern and there is reason to believe that relations between China and the West might deteriorate further. In this connection, Chinese EVs in particular are increasingly seen as a security concern in the West.

The most pressing issue is probably that the stream of data sent back to China might allow the Chinese government to use EVs abroad for intelligence gathering, including spying on individuals and mapping patterns of movement and physical locations, and that the data collected might be used for training military-grade AI and other applications. More than individual data is at risk as large-scale data collection could also reveal crucial information about collective behaviour, traffic patterns and the flow of goods in a target society. In this context it is generally assumed that the Chinese government, through its National Intelligence Law and by other means, will be able to compel Chinese carmakers to hand over sensitive data.

There is also concern about the use of vehicles for active sabotage and attacks in a situation of increasing China-West conflict. US Secretary of Commerce Gina Raimondo voiced these concerns in May 2024: "You can imagine the most catastrophic outcome theoretically if you had a couple million cars on the road and the software were disabled". For its part, China has already taken steps to restrict Tesla cars from entering sensitive government-related areas in China due to concerns over data collection. These restrictions demonstrate that China is aware of the risks posed by connected vehicles and their data collection capabilities.

Some argue that there are national security risks associated with Chinese technologies even at the component level. It has been suggested that the main security issues with Chinese EVs are linked to the cellular IoT (Internet of Things) modules (CIMs) that enable internet connectivity within vehicles. These CIMs, which are ubiquitous in many everyday items, allow vehicles to access over-the-air software updates and are critical for the operation of most connected vehicle systems. China's market position in this field increasingly resembles a monopoly, and companies such as Quectel and Fibocom lead the global market. At the end of 2022, Chinese firms accounted for 64 percent of global CIM sales, a market share that equates to 75 percent of IoT connections.

Critics who see CIMs as the main digital vulnerability, such as the British analyst, Charles Parton, argue that eliminating all security risks connected to Chinese intelligence gathering would require "ban[ning] any Chinese module in any vehicle". They warn that any vehicle equipped with a Chinese-made CIM could, in theory, have its data "sucked up" by the Chinese Communist Party, and that these CIMs could be manipulated to disable vehicles remotely. However, it should be noted that there is no direct public evidence of the Chinese government extracting data from CIMs at present. In general, Chinese companies would have to be prepared to risk the significant legal and reputational losses that any espionage or sabotage would entail if discovered. A willingness to bear such risks, among China's companies or its government, should by no means be taken for granted.

Regulatory responses in the United States and the European Union

In response to these risks, governments—primarily the US Government—have begun to investigate the potential data and cybersecurity threats posed by Chinese electric vehicles

and other connected cars. The US Department of Commerce announced an investigation into the risks in February 2024, and in May 2024 the Biden administration announced 100 percent tariffs on Chinese-made electric cars. The primary justification for this measure was to protect US manufacturers from unfair trading practices but the United States is now clearly reacting to more far-reaching concerns over Chinese technology, as demonstrated by more recent proposals aimed at Chinese hardware and software components.

In September 2024, the US Department of Commerce proposed a prohibition on the sale and import of connected vehicles containing hardware and software "with a sufficient nexus" to China (as well as Russia), in order to prevent "malicious access". If implemented, this restriction would also affect the European car sector, as it would need to move away from Chinese suppliers in order to maintain access to the US market. These restrictions on Chinese software will take effect in 2027, while hardware restrictions are to be applied from 2030. The hardware rule would include CIMs. Such measures would provide an advantage to any European manufacturers that are less reliant on Chinese technology but create challenges for brands that have significant operations in China or, like Sweden-based Volvo Cars, Chinese owners. The Canadian Government is also considering measures against Chinese connected vehicle technology, and the issue is being debated in Australia and the UK.

Things have been moving more slowly in Europe. The EU imposed new tariffs on Chinese EVs in July 2024, increasing them to a range from 27.4 percent to 47.6 percent, depending on the manufacturer. However, these tariffs were motivated by concerns over unfair trading practices rather than national security. In December 2023, the European Commission announced that it was prioritizing investigating the cybersecurity aspects of connected and automated vehicles, including EVs. In September 2024, it was reported that the Commission's security assessments might lead to an "ICT supply-chain toolbox" that resembles the existing 5G security toolbox, but as yet no concrete proposals have been tabled.

Policy recommendations for the EU

How to address these security concerns is ultimately a political question. Much depends on the long-term development of relations between China and the EU, and the perceived level of threat from China. Nonetheless, existing security vulnerabilities suggest that there should be at least minimum protection to prevent Chinese intelligence gathering and malicious influence against European citizens and governments.

1. The EU should launch its own investigation into the security risks associated with Chinese EVs.

2. Following the pattern of the partial restrictions on Teslas in China, Chinese vehicles should be prohibited for personnel working in politically sensitive or security-related areas, even for their private use. The use of Chinese CIMs should also be prohibited in the national security sector, where this is not already the case.

3. The EU could consider requiring Chinese manufacturers to store any data collected from cars sold in the EU within the Union, with the threat of imposing corporate fines if vehicle data is found to have been transferred back to China. This would mirror the corresponding requirements on personal information and important data in China's own Cybersecurity Law.

Alexis von Sydow

Alexis von Sydow is an analyst at the Swedish National China Centre.

About the Swedish National China Centre

The Swedish National China Centre was established in 2021 as an independent unit at the Swedish Institute of International Affairs (UI). The Centre conducts policy-relevant research and aims to contribute to a long-term improvement in the state of China-related knowledge in Sweden. UI's publications undergo internal quality control. Any views expressed are those of the author.