RSIS COMMENTARY

3 February 2026

Vehicles with OTA Capabilities – A Threat to National Security?

Gabriel Lim Hong Liang

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 020 – 3 February 2026

Vehicles with OTA Capabilities – A Threat to National Security?

By Gabriel Lim Hong Liang

SYNOPSIS

This commentary sheds light on the national security risk posed by vehicles equipped with over-the-air (OTA) capabilities. Such vehicles can send and receive signals/information to and from external sources, which, in theory, makes them vulnerable to being remotely controlled or influenced.

COMMENTARY

On 5 November 2025, Norwegian bus company Ruter tested two electric buses – one from Chinese bus manufacturer Yutong and one from the Netherlands. This was to understand how these buses collected data, given the risk of remote access. Ruter concluded that Yutong's buses posed a national security risk, as their over-the-air (OTA) capabilities – systems that allow devices to transmit and receive data remotely – could compromise them. An emerging concern is the need for greater awareness, alongside appropriate policy responses, to address the potential dangers posed by vehicles with OTA functionality to Singapore's national security.

Ruter's Findings

Ruter concluded that the Yutong buses' OTA capabilities meant the manufacturer had direct access to their core systems, such as the buses' batteries and power supplies, allowing Yutong to disable them remotely at will. Ruter concluded that this issue posed a national security concern for Norway but also acknowledged that the level of integration among the various electronic systems of Yutong buses was limited and was confident that they could "delay the signals to the bus, [and] gain insight into the updates being sent". They noted that such systems were already being implemented.

Countries Respond

Ruter's findings prompted follow-up investigations in Denmark and Britain, as they were in the process of implementing or already had Yutong-made buses in their public transport fleets.

With 469 Chinese-made buses in its public bus fleet (262 of which were manufactured by Yutong), Denmark resonated with Norway's concerns and would be "urgently studying" this "security loophole".

Alongside the two Nordic countries, Britain expressed similar concerns regarding the hundreds of Yutong/Chinese-made buses plying its roads. It launched investigations on 10 November 2025 and, on 3 January 2026, concluded them, aligning with Ruter's view that it is technically possible to disable its buses remotely. However, given the lack of evidence of such sabotage, acquisitions and the use of Chinese-made buses in Britain remain unaffected.

Yutong's Response

Yutong, which is partially owned by the Chinese government, issued a response calling Ruter's findings "technically impossible". It provided an assurance that, while its vehicles feature OTA connectivity for diagnostics and software updates, there is no physical connection between such systems and safety-critical systems such as steering, propulsion, or braking.

Yutong also made clear that the data collected by its buses in the European Union is stored on Amazon Web Services servers in Frankfurt, is used exclusively for maintenance and performance optimisation, and is protected by encryption and restricted access protocols.

The Chinese bus company also stated that all OTA updates are made with the operator's explicit approval and are limited to comfort, interface, diagnostic functions, and do not affect vehicle control systems. It also noted that certain systems, such as those that regulate cabin temperature, are managed entirely by local operators, with no direct access from Yutong.

As of 2025, Yutong is the world's largest electric bus manufacturer. It has approximately 110,000 buses operating in 130 countries and regions across Asia, Africa, Latin America, the Middle East, and Europe. Yutong is also widely regarded as a pioneer in environmentally sustainable technologies, having launched its Net Zero Forest initiative in April 2025. By no means a mere supplier of public buses, Yutong is arguably an important component of Chinese soft power.

Yutong Buses in Singapore

Responding to Ruter's study, Singapore's Land Transport Authority (LTA) issued a statement on 17 November 2025, assuring the public that the twenty local Yutong buses had no OTA capabilities, had been functioning as intended since 2020, and were all locally operated. The LTA reiterated that it requires all its contractors to

adhere to “strict data protection measures”. It had also met with Yutong as well as two other Chinese bus manufacturers, BYD and Zhongtong, regarding the issue.

On 12 January 2026, in response to questions in parliament, Acting Minister for Transport Jeffrey Siow noted that the LTA had begun collaborating with cybersecurity agencies on improving the safety of OTA updates. He also reassured the public that Singapore’s public buses were equipped with certified cybersecurity controls to detect and counter intrusions, and that authorised personnel on-site using a physical, wired connection were needed to update their software.

The Risks Posed by Vehicles with OTA Capabilities

While a relatively new area of national security concern, the data-collection capabilities of such technologies and the potential risks they pose are well known.

Vehicles with OTA functionality likely gather extensive data on our lives – such as our driving habits and the places we frequent. While data laws exist, how data is ultimately used by external actors (state or otherwise) is unlikely to be fully known to the target country.

While the notion of remotely compromising a vehicle through its external connections may seem within the realm of science fiction, Ruter’s investigation into Yutong’s buses has shed light on that very possibility, given how prevalent OTA functionality is across all kinds of vehicles. These systems already allow a vehicle’s core functionalities to be accessed, such as Tesla’s “Summon” feature, which lets an owner remotely control their car.

An external actor could sabotage a country’s public transport and/or road infrastructure to soften it up for an incoming attack, test a target country’s defence systems, or simply as a response to any action it deems against its interests. An actor with such capabilities may not even need to disable a target country’s transportation network to compel it to act in a certain way – the threat alone of such a comprehensive act of sabotage may suffice.

Singapore’s Response to the Threat

In response to technologies with OTA capabilities becoming a national security concern, some countries have implemented restrictions or even outright bans on specific technologies (such as the United States’ restrictions on the import and sale of certain Chinese-made telecommunications equipment).

Singapore’s hub-of-hubs economic strategy makes such a policy far less feasible. Alongside the potential to sour relations with trading partners, restricting such vehicles would likely have detrimental economic impacts that outweigh the national security assurances such a measure may provide (if any).

Nevertheless, Singapore to some extent already implements countermeasures that indirectly mitigate this threat, as it diversifies its acquisition of certain technologies that are critical to core state functions and develops some of them in-house.

However, policy measures can be beefed up to face this emerging threat, such as legislation on vehicles with OTA capabilities. As we already have legislation specifically addressing the testing of autonomous vehicles that rely on OTA updates, building on these existing laws to compel automakers to provide greater transparency on their vehicles' OTA systems (and to restrict them where necessary) is likely a feasible approach.

Conducting tests akin to Ruter's could also be another key measure to understand better the risks that vehicles with OTA updates pose to national security. Comparative tests of vehicles with OTA functionality from different makes, models, and countries could help us understand how manufacturers utilise this technology and which applications of these systems are of concern.

Increased public awareness of this issue is also crucial if Singapore is to develop social resilience and a sense of vigilance towards such technologies. This could help the public adopt practices, such as raising the alarm when suspicious changes or updates occur in a vehicle, turning off systems like GPS and other telemetries when not in use, and informing and/or assisting authorities in identifying and combating potential threats.

Addressing the threat posed by vehicular OTA systems to Singapore's security is urgent and complex, as the challenges of countering its dangers without adversely impacting our lives will require a whole-of-society approach. This episode highlights how technology can pose unique national security challenges, which potential adversaries can exploit to advance their own interests.

Gabriel Lim is a Senior Analyst with the National Security Studies Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. He was formerly a Research Assistant with the Institute of Policy Studies at the Lee Kuan Yew School of Public Policy, Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.