DGAP MEMO
German Council on Foreign Relations e. V.
No. 50
November 2025

THE GEOPOLITICS OF BATTERIES

Connected Vehicle Cybersecurity: The EU Must Consider Non-technical Risk Factors

Dr. Valentin Weber, Senior Research Fellow, Center for Geopolitics, Geoeconomics, and Technology, DGAP; Maria Pericàs Riera, Fellow, Internet Society

Connected vehicles are revolutionizing mobility – but also introducing cybersecurity risks. These vehicles raise concerns over foreign access and interference, particularly from China. While EU measures like the General Safety Regulation set out technical guidelines to secure this ecosystem, they fall short of making non-technical risk factors a core security principle. To be coherent with its 5G Toolbox, the EU urgently needs to include those in upcoming regulations.

Concerns over security risks linked to connected car technology are slowly gaining traction. In October 2024, the German Association of the Automotive Industry (VDA) stated that "ensuring maximum security is in the best interests of the German automotive industry. The VDA is therefore pursuing a proactive approach to preventing cyber attacks and protecting connected vehicles." Given the vast amount of data that connected vehicles collect, ranging from location tracking to driver behavior analytics, the potential for foreign access and exploitation of such data should be a pressing security issue for the EU and Germany. In addition to monitoring geographic and behavioral data, electric vehicles also track the charge and temperature of their batteries through integrated battery management systems (BMS). It is these battery management systems that allow for a digital interface with a battery, providing an avenue for cyber-based disruption or sabotage.

The EU already recognizes cybersecurity as a key issue in the automotive sector. Currently, Regulation (EU) 2019/2144, also known as the General Safety Regulation (GSR), sets cybersecurity requirements for vehicle manufacturers. It aligns with the United Nations Economic Commission for Europe Regulation No. 155 and the EU's measure to generally protect network and information systems, Directive 2022/2555, also known as NIS2. Compared to its legislative ancestor NIS, NIS2 expands the number of entities that have to comply with strict cybersecurity regulations. With mandatory compliance for all new vehicles as of July 2024, the GSR establishes mandatory safety requirements for motor vehicles, their trailers, and the systems, components, and technical units they use. According to this regulation, vehicle manufacturers must demonstrate how the supply chain was managed and how the supplier components integrate into the vehicle's overall cybersecurity architecture. This includes suppliers setting cybersecurity measures to prevent the manipulation of vehicle parameters, such as battery temperature. An example that illustrates the effects of this regulation is Porsche's decision to discontinue its 718 combustion engine models in the EU and some other countries because it was not financially feasible to adapt the connected components of those cars to meet its cybersecurity standards. However, the GSR regulation omits an important aspect: it does not take the manufacturer's country of origin into consideration.

This regulatory gap raises concerns about potential vulnerabilities that could be exploited by strategic competitors such as China – for example, through Chinese software or hardware components that are integrated into vehicles at different stages of production or deployment. Because the EU's GSR and NIS2 only set out technical

cybersecurity baselines, they fall short here. Therefore, this DGAP Memo analyzes how such geopolitical risks can be addressed by additional regulations that include non-technical risk factors such as ensuring the trustworthiness of the suppliers of cars or components like battery management software.

BERLIN AND BRUSSELS ARE SLOWLY MOVING IN THE RIGHT DIRECTION

In response to these concerns, the EU has been developing a voluntary toolbox to protect supply chains related to information and communication technologies (ICT) that has been proposed by member states but remains unpublished at this writing. This toolbox would mirror the EU's existing 5G security toolbox, which outlines measures for mitigating cyber espionage and interference by providing guidance to assess the implications of using foreign high-risk ICT suppliers. The ICT Supply Chain Toolbox might be integrated into a revision of the Cybersecurity Act, which would make it a binding document for regulators and operators in the EU. Germany appears to be on the more security-minded side of EU member states while Hungary and Spain take a more doveish stance in regulating high-risk suppliers.

Germany's position on supply chain regulations highlights a potential threat to its regulatory approach in the cyber realm. In fall 2025, the German government weakened its Supply Chain Act (*Lieferkettengesetz*), a law requiring companies to ensure that human rights and environmental standards are upheld in their global supply chains, by suspending reporting obligations under that act. German business groups had criticized it as an excessive burden.

This move raises questions about whether German and other EU companies will be willing to adopt further cybersecurity regulations related to the supply chain. Given that pressure from industry helped weaken Germany's *Lieferkettengesetz*, there is a risk that German and European companies may push for similar flexibility in the ICT Supply Chain Toolbox by arguing that strict cybersecurity supply chain requirements could undermine their competitiveness. However, in the current geopolitical environment, there is likely to be more political appetite for imposing supply chain regulations on industry that relate to cybersecurity rather than human rights.

The EU's ongoing efforts to address cybersecurity in connected vehicles represent a crucial step, but further development is needed. While future initiatives like the ICT Supply Chain Toolbox offer hope, their success depends on consistent member state implementation – a challenge highlighted by the inconsistent adoption of the 5G toolbox and the potential weakening of supply chain regulations. Without a unified and comprehensive framework, the EU risks significant vulnerabilities in its connected vehicle ecosystem.

RECOMMENDATIONS FOR THE EU AND GERMANY

How can a comprehensive cybersecurity approach be achieved? Since the ICT Supply Chain Toolbox is broader in nature, the EU should draft an additional regulation, specifically on the issue of connected vehicles. The new regulation should integrate the following recommendations.

First, Germany and the EU should draft a binding rule at home that is similar to the one regarding connected vehicle cybersecurity published by the US Department of Commerce's Bureau of Industry and Security. Accordingly, the EU regulation should restrict the use of Chinese and Russian components in connected vehicles that are particularly exposed to sabotage and espionage, e.g., Wi-Fi connectivity and advanced driver assistance systems. The US rule, which took effect on March 17, 2025, explicitly bans cars and components with China and Russia as their country of origin. This is due to the geopolitical risk that comes from both of their governments, which have indicated long-term behavior that is contrary to US national security interests. The rule lays out the threat as "undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of" digital technology. Similarly, one of the authors of this DGAP Memo has warned that China and Russia could have what he called "privileged access" to connected vehicles through their role as suppliers.

Second, when the EU creates its equivalent of the US connected vehicle cybersecurity rule, it should be more precise in the wording of what is banned. The US rule identifies Wi-Fi, cellular and satellite connectivity, and Bluetooth as the components through which the vehicle communicates with the outside world. These components also include the operating system itself; telematics systems that visualize the data they have collected from sensors and engine and driving behavior; advanced driver assistance systems such as emergency brake assist; automated driving systems; and battery management systems that monitor and control battery charging and use. In a statement, the VDA noted that auxiliary heaters and autonomous driving systems of levels 1 to 2+ should be omitted from such a binding document because they do not pose grave security risks. An EU regulation would benefit from such specificity in wording as it allows risk to be assessed in a more granular way, therefore reducing costs for industry.

Third, Germany and the EU need to move fast. Unlike in 5G, Chinese vendors do not yet have a larger presence on German and European territory in the connected vehicle space. The longer Europe waits, the costlier the expunging of risky components will become. With every day, month, and year, the market

share of Chinese car companies, such as BYD, may grow – as may that of Chinese providers of hardware and software components due to joint ventures of German carmakers with companies such as XPeng and Brilliance Auto Group. The pronouncement of plans for a binding EU rule on connected vehicle cybersecurity could already be a wake-up call to German carmakers. A more risk averse approach to China would also be in line with the policy announcements made by German Chancellor Friedrich Merz, head of the conservative Christian Democratic Union (CDU), who recently said that any German investment in China comes with a "great risk."

Fourth, Brussels and Berlin should closely discuss and fine tune any regulation with key partners. These include Italy and France; Japan, South Korea, and the major other car manufacturing countries; and the European Union more broadly. This should be done not only to determine the content of the rule but also the timing of its pronouncement and when it will take effect.

Finally, Germany should continue to make trust a central component of supply chains related to any future mobility technology, including drones. Drones will pose a particularly daunting challenge to de-risk since China so overwhelmingly dominates this sector.

The sweeping new export controls China issued in October 2025, which cover much of the battery value chain, underscore the need for energy storage sovereignty in Europe. China made the move amid mounting turmoil in Europe's battery sector marked by the bankruptcies of high-profile firms such as Northvolt and BMZ Germany. In response, DGAP's Center for Geopolitics, Geoeconomics, and Technology has launched this series of memos that examines the geopolitics of batteries.

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für Auswärtige Politik e.V.

ISSN 2749-5542

Editing Helga Beck

Layout Luise Rombach