

(English version)

Question for written answer E-003112/26
to the Commission
Christine Anderson (ESN)
(23 July 2026)

Subject: Hybrid threats and foreign-controlled charging infrastructure

On 24 February 2026, the partly publicly-owned German energy company EnBW concluded a multiannual agreement with XCharge for high-power charging stations. EnBW operates more than 8 000 fast-charging points and plans to expand its network to up to 20 000 by 2030.

XCharge was founded in Beijing. According to its US Securities and Exchange Commission (SEC) filings, its chief executive officer (CEO) and its chair/chief technology officer (CTO) control approximately 81.9% of the voting power through Class B shares, while holding approximately 31.2% of the share capital.

Operators of recharging points are expressly covered by the energy provisions of the Network and Information Systems (NIS 2) Directive, subject to its scope criteria. The Commission has also identified strategic dependencies, unauthorised access to operational data and remotely triggered disruptions as risks arising from connected energy equipment. It has restricted EU funding for projects using solar inverters from high-risk suppliers.

1. Beyond the general cybersecurity and supply-chain obligations under the NIS 2 Directive, does EU law require the assessment of suppliers' ultimate control, third-country legal obligations, data access and remote software-update or maintenance capabilities?
2. Can charging equipment comply with the EU cybersecurity framework where persons exercising decisive control over the supplier retain remote-access or update capabilities and are subject to the laws of a third country presenting elevated security risks?
3. Will the Commission apply supplier-security and funding restrictions to networked charging infrastructure equivalent to those applied to solar inverters, or explain why charging networks should be treated differently?

Submitted: 23.7.2026

Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(2 October 2026)

The proposal for revision of the Cyber Security Act ⁽¹⁾, currently under negotiation by co-legislators, sets out an objective and risk-based framework to address risks related to foreign interference and dependencies in the ICT Supply Chain in NIS 2 sectors ⁽²⁾.

For charging infrastructure specifically, the Risk Assessment on Connected and Automated Vehicles (CAV ⁽³⁾) recommends that Member States apply the ICT Supply Chain Security Toolbox to 'CAVs and related charging infrastructure', including assessment of critical suppliers, multi-vendor strategies, reducing dependencies on high-risk suppliers and, where appropriate, restricting or excluding high-risk suppliers from critical supply chains. Risk assessments are legally of non-binding nature.

The proposal for revision of the Cyber Security Act ⁽⁴⁾ sets out that the high-risk suppliers, as defined in the proposed act, shall not be entitled to participate in any activities under EU funding programmes and instruments implemented in direct and indirect management in accordance with Article 136 Regulation (EU, Euratom) 2024/2509 and EU sector-specific rules as well as in any EU funding activities implemented in shared management in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with the regulation.

⁽¹⁾ <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>.

⁽²⁾ <https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks>.

⁽³⁾ <https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>.

⁽⁴⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0011>.