

(English version)

**Question for written answer E-000889/25
to the Commission
Kosma Złotowski (ECR)
(3 March 2025)**

Subject: Chinese wind turbines as a threat to energy security

In 2024, the Commission initiated an investigation into Chinese suppliers of wind turbines in Spain, Greece, France, Romania and Bulgaria, due to suspicions of Chinese state subsidies. This was motivated by concerns that the domestic industry may be affected by the influx of inexpensive imports, which could lead to its collapse. It is noteworthy that China has already dominated the photovoltaic industry in Europe and is expanding aggressively into other markets, including the electric vehicle market.

In addition to these highly controversial and questionable issues, a report commissioned by Germany's Ministry of Defence, prepared by the German Institute for Defence and Strategic Studies, states that China may deliberately delay projects, remotely disable turbines, collect confidential information on energy security and pose a serious threat to cybersecurity.

1. What is the status of the Commission's 2024 investigation into wind turbine subsidies, and can any conclusions be drawn yet?
2. Is the Commission contemplating the potential of a comparable threat involving market manipulation, data theft, or even the control of electric cars produced by Chinese manufacturers?
3. Does the Commission concur with assertions that excessive reliance on China amplifies the risk of cyberattacks, which could result in the cessation of renewable energy production from wind turbines, and therefore would the Commission recommend that the Member States consider excluding non-EU countries from tenders?

Submitted: 3.3.2025

**Answer given by Executive Vice-President Ribera on behalf of the European Commission
(12 May 2025)**

The Commission's preliminary review into potential distortions in the internal market linked to potential foreign subsidies in the wind sector is ongoing. At this stage, it is too early to draw any conclusions.

Critical technologies used in connected and automated vehicles (CAV) could have cybersecurity associated risks. They can potentially be remotely accessed and manipulated. They can also potentially collect and store sensitive data about citizens, infrastructure, and external environments which could be exposed to malicious actors. Member States, together with the Commission and European Union Agency for Cybersecurity (ENISA), are currently working on a risk assessment on CAV within the framework of Article 22 of the Network and Information Systems (NIS) 2 Directive with the objective to identify and assess cybersecurity risks posed by those vehicles, taking into account both technical and non-technical factors. The risk assessment will be finalised in the coming months.

The Commission is taking steps to ensure that the deployment of energy from renewable sources includes appropriate cybersecurity risk management measures. Article 26(1)(a)(ii) of the regulation (EU) 2024/1735 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ⁽¹⁾ provides that auctions to deploy renewable energy sources shall include pre-qualification criteria related to cybersecurity and data security.

Additionally, the Commission is conducting a cybersecurity risk assessment for wind energy infrastructure, in collaboration with the industry, following Action 5 mentioned in the Wind Power Action Plan ⁽²⁾.

⁽¹⁾ Regulation (EU) 2024/1735 of 13 June 2024 on establishing a framework of measures for strengthening Europe's Net-Zero Technology manufacturing ecosystem and amending Regulation (EU) 2018/1724 (Net-Zero Industry Act).

⁽²⁾ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions — European wind power action plan, (COM(2023)0669 final).