

(English version)

**Question for written answer E-002219/25
to the Commission
Beatrice Timgren (ECR)
(3 June 2025)**

Subject: Risks linked to hidden communication modules in solar inverters

A recent investigation has revealed that solar inverters manufactured by Chinese companies and deployed across Western markets may contain communication modules capable of transmitting data without the knowledge of the user ⁽¹⁾. These hidden modules, thus far only discovered in models exported to US markets, raise serious cybersecurity and sovereignty concerns. Such devices are reportedly installed in the products without being listed in the product documentation. This could potentially enable remote shutdowns and data exfiltration.

Given the above:

1. Is the Commission aware of these findings, and has it initiated an investigation into the security implications of Chinese-made inverters installed within the EU?
2. What steps is the Commission taking to assess and mitigate risks to energy infrastructure from Chinese-controlled hardware and software?
3. Will the Commission consider adjusting existing EU security standards or certification procedures to ensure that solar inverters and related components are subject to checks for hidden communication capabilities?

Submitted: 3.6.2025

**Answer given by Ms Virkkunen on behalf of the European Commission
(29 July 2025)**

The Commission is aware of the findings mentioned and is planning to conduct a risk assessment for solar energy infrastructure, including inverters, as announced at the SolarPower Summit last March ⁽¹⁾.

The information and communications technology (ICT) supply chain security remains high on the EU agenda. In the recently adopted ProtectEU Strategy ⁽²⁾, the Commission highlights the need to avoid critical dependencies and de-risk EU ICT supply chains from high-risk suppliers.

Union-level risk assessments on the cybersecurity of digital infrastructures and supply chains are conducted by the Network and Information Systems Cooperation Group, supported by the Commission and the European Union Agency for Cybersecurity (ENISA), pursuant to Article 22 of the NIS2 Directive ⁽³⁾.

Solar energy infrastructure is one of the technologies identified by the Commission and the Member States for one of these Union-level risk assessments. The Commission will thoroughly evaluate the findings of the planned risk assessment for solar energy infrastructure.

Policy choices regarding cybersecurity standardisation and certification, informed by this risk assessment, cannot be anticipated at the current stage of the process.

In addition, within the revision of the Cybersecurity Act, the Commission will also look at the ICT supply chain security and will consider how to address critical dependencies and how to de-risk EU ICT supply chains and ensure their security.

¹ Reuters, 'Rogue communication devices found in Chinese solar power inverters', 14 May 2025, <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14>.

⁽¹⁾ <https://www.solarpowereurope.org/news/shining-moments-from-the-solar-power-summit-day-2>.

⁽²⁾ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: a European Internal Security Strategy.

⁽³⁾ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).