European Parliament

Brussels, 24 October 2025

Dear Executive Vice-President Virkkunen,
Dear Commissioner Jørgensen,

We write to you with deep concern about the Commission's approach to addressing risks stemming from high-risk vendors, particularly in the field of solar (PV) inverters. We urge you to propose immediate and binding measures to restrict high-risk vendors from our critical infrastructure.

Huawei, designated as a high-risk vendor by the Commission, accounted for over 115 GW of Europe's solar inverter market up to 2023. It is one of six Chinese vendors that collectively control more than two-thirds of the market (219 GW) in Europe.[1] And our dependency is deepening: in 2024, 80% of all new PV inverter capacity installed in Europe originated from China.[2]

Lithuania has already banned remote Chinese access to solar and wind devices.[3] More recently, the Czech and German national cyber security agencies NUKIB and BSI have warned of the risks posed by Chinese-linked technologies in critical sectors, highlighting Chinese PV inverters as a high-risk technology for supply chain attacks on our grid, and urging the use of non-technical risk factors to address these risks.[4] Chinese authorities recognise these risks, meaning that European inverters are de facto not allowed into their grid, on the basis of cybersecurity grounds. Europe should adopt a similar approach.

The Commission has dedicated considerable effort to risk assessments, highlighting the risks posed by high-risk vendors in our critical infrastructure. However, concrete proposals have yet to materialize.[5] When the ongoing studies are completed and potential legislation is tabled, as much as two years may have passed. By that time, Europe risks having lost its remaining PV inverter manufacturers. Western companies are drastically losing market share in Europe, though they currently still retain the capacity to meet European demand. If one of them succumbs to unfair competition from China, the Union could soon be left without any non-Chinese alternatives

Binding legislation to restrict risky vendors in our critical infrastructure is urgently required, either through the revision of the CSA or elsewhere. Vice-President Virkkunen has already shared her dissatisfaction with the lackluster implementation of the voluntary 5G toolbox, calling for stronger measures, and considering binding legislation.[6] Compared to telecom, the secure management of Europe's power grid is inherently a Union-wide issue: the failure of a single link has the potential to trigger cascading disruptions across the continent.

Until binding legislation is in place, a temporary framework should be established to restrict risky vendors from our energy infrastructure. Many precedents already exist, such as the 5G Toolbox that can include non-technical risk factors, such as the NZIA cybersecurity criteria.[7] The German energy association BDEW has also proposed blacklisting or whitelisting of (un)trustworthy companies.[8]

Without immediate and binding EU action, Europe risks not only its energy security but also the viability of all remaining European manufacturers in this sector. We look forward to your urgent response and a clear timeline for legislative action.

Yours sincerely,

Bart Groothuis (Renew)
Miriam Lexmann (EPP)

[1] Solar Power Europe, Solutions for PV Cyber Risks to Grid Stability.
[2] S&P, Global Commodity Insights.
[3] Reuters, Rogue communication devices found in Chinese solar power inverters.
[4] NUKIB, Warning against the Transfer of the data to and Remote Administration from People's Republic of China; BSI, Positionspapier: Cybersicherheit im Energiesektor Deutschlands.
[5] European Commission, Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors (July 2024) and another Risk assessment announced by for the solar industry in response to written questions.
[6] Euractiv, Tech Commissioner Virkkunen favours regulation over directive for EU's telecom law reviewl.
[7] The NZIA cybersecurity pre-qualification criteria assess whether a manufacturer is subject to a jurisdiction requiring disclosure of software vulnerabilities to state authorities before they are known to be exploited; and whether it is based in a jurisdiction from which malicious cyber activities have been carried out against the Union or its Member States (Article 5 of Commission Implementing Regulation (EU) 2025/1176).
[8] BDEW, Positionen des BDEW Bundesverband der Energieund Wasserwirtschaft und VKU Verband kommunaler Unternehmen zum § 41 BSIG: (p.9).

bart.groothuis@europarl.europa.eu