

(English version)

Question for written answer E-002483/25
to the Commission
Michał Wawrykiewicz (PPE)
(20 June 2025)

Subject: Prevention of power outages

In reaction to the power outages in Spain and Portugal on 28 April 2025 it is clear that the EU needs to strengthen the security of its critical infrastructure. The blackout lasted for 36 hours and its impact on the Spanish economy alone is estimated to be EUR 1.6 billion. The outage had a knock-on effect on the mobile network. Around 150 flights were cancelled in both countries due to the outage. In Spain, download speeds in some areas fell by as much as 85%, while in Portugal, speeds in regions such as Porto and Vila Real dropped by 90%. Unfortunately eight people have died as a result of the outages.

1. What mechanisms will the Commission employ to protect critical infrastructure at the EU level?
2. Does the Commission plan to review and update the directive on the Resilience of Critical Entities (2022/2557) or any other relevant provisions of EU law concerning the security of critical infrastructure?
3. What measures are being considered by the Commission to enhance the EU's capacity to prevent, detect and respond to cyberattacks and acts of sabotage targeting critical infrastructure, particularly in the energy, transport and telecommunications sector?

Submitted: 20.6.2025

Answer given by Mr Brunner on behalf of the European Commission
(7 August 2025)

The EU has strengthened the legislation on critical infrastructure, both from a physical and cyber resilience perspective with the directive on the Resilience of Critical Entities ⁽¹⁾ and the directive on measures for a high common level of cybersecurity across the Union (the NIS 2 Directive) ⁽²⁾. ProtectEU, the new European Internal Security Strategy ⁽³⁾, streamlines EU action in this area.

The Council Recommendation on critical infrastructure resilience ⁽⁴⁾ led to the conduct of stress tests in the energy sector.

The review of the energy security of supply framework by 2026 will assess and update the existing EU energy security framework to make it suitable for decarbonisation, as well as to better address emerging risks, including natural hazards or man-made threats.

As regards cybersecurity, the EU has a comprehensive framework in force with the NIS 2 Directive and the Cyber Resilience Act ⁽⁵⁾, which focuses on cybersecurity requirements for products with digital elements.

The EU also has specific technical binding rules for cybersecurity in the cross-border electricity flows in the EU and neighbouring countries.

Cybersecurity risk assessments are underway in critical sectors, including energy, under Directive (EU) 2022/2555 ⁽⁶⁾. A risk assessment for wind under the wind package is being carried out, and a similar assessment will be carried out for solar energy infrastructure.

The Commission also adapted the first-ever EU network code on cybersecurity for the electricity sector in March 2024 and adopted, with the High Representative/Vice-President, the EU Action Plan on Cable Security in February 2025 ⁽⁷⁾.

In addition, the European Preparedness Union Strategy ⁽⁸⁾ enhances the EU's preparedness and readiness for future crises.

⁽¹⁾ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, pp. 164-198.

⁽²⁾ 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), OJ L 333, 27.12.2022, pp. 80-152.

⁽³⁾ COM(2025) 148 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148>.

⁽⁴⁾ Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure 2023/C 20/01, OJ C 20, 20.1.2023, pp. 1-11.

⁽⁵⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>.

⁽⁶⁾ See footnote 2.

⁽⁷⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0009>.

⁽⁸⁾ Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, JOIN(2025)130 final.