

Question for written answer E-003667/2025

to the Commission

Rule 144

Borja Giménez Larraz (PPE), Nicolás Pascual de la Parte (PPE)

Subject: Cyberattack on check-in providers at European airports and resilience against hybrid threats and external actors

Since 19 September 2025, a cyberattack on check-in and boarding systems provider Collins Aerospace has forced airports such as Brussels and Berlin to operate manually, leading to delays and cancellations affecting hundreds of thousands of passengers.

The European Union Agency for Cybersecurity (ENISA) has labelled it a third-party cyberattack. The Commission has noted that neither aviation safety nor traffic control was compromised and that it is coordinating with authorities and bodies, but the number of operational incidents is considerable.

The attack demonstrates the reliance on critical suppliers and the need to effectively implement the NIS 2 Directive (Directive (EU) 2022/2555) and the CER Directive (Directive (EU) 2022/2557).

In light of the above:

1. Does the Commission intend to carry out stress tests, joint exercises and cross-border contingency plans – with ENISA (and Eurocontrol/AESA) – for failures or attacks on airport IT providers?
2. How does the Commission assess hybrid security risks to air transport and what action will it prioritise to mitigate those risks with Member States?
3. Does the Commission intend to provide guidance so that – in Spain and the EU – security service procurement includes risk assessments to place restrictions on awards to high-risk suppliers from third countries, including China, where appropriate?

Submitted: 22.9.2025