

(English version)

**Question for written answer E-000973/26
to the Commission
Juan Ignacio Zoido Álvarez (PPE)
(9 March 2026)**

Subject: Cybersecurity breach in Spain

On 28 February 2026, several media outlets reported that the Spanish National Police and Civil Guard systems had been hacked, with data linked to credentials of agents from both entities being stolen. The next day, it emerged that the same cybercriminals had also accessed the personal information of members of Spain's National Security Council, including the President of the Government, several ministers and the Chief of Defence Staff.

These events occurred against a backdrop of a sharp increase of cyberattacks in Spain — cyberattacks have increased by 26% over the past year, with over 122 000 incidents in 2025. Despite this, Spain has still not transposed the NIS 2 Directive, which aims to reinforce the cybersecurity and resilience of the EU's critical infrastructure.

In light of the above:

1. In the Commission's view, do these kinds of breaches pose a threat to EU security?
2. What support measures does the Commission envisage to make Member States more resilient to these kinds of attacks?
3. Does the Commission believe that Spain's failure to implement the NIS 2 Directive leaves the country and its companies in a vulnerable position and that the Spanish Government should enforce this transposition?

Submitted: 9.3.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(19 May 2026)**

Directive (EU) 2022/2555 ⁽¹⁾ aims to increase the cybersecurity of entities operating in 18 critical sectors, including public administration.

Under this directive, Member States must ensure that certain public administration entities take cybersecurity risk-management measures and report significant incidents.

This directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement.

In the current global threat landscape, cyberattacks disrupt critical infrastructure and economic stability. Robust cybersecurity is paramount and the transposition of Directive (EU) 2022/2555 a strategic imperative. Spain must urgently advance with the full transposition of this directive.

An infringement procedure ⁽²⁾ has already been initiated by the Commission in this respect. The urgency of the transposition is not just about the obligation under the law; it is fundamental to reinforce the cyber standards of our critical infrastructure.

The Commission remains fully committed to assisting Member States' efforts and helping them overcome any challenges in the transposition process, while respecting the ongoing infringement processes concerning the Member States that have not yet notified full transposition of Directive (EU) 2022/2555.

⁽¹⁾ 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 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

⁽²⁾ INFR(2024)0270 Lack of transposition of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union by Spain, source: https://ec.europa.eu/commission/presscorner/detail/en/inf_25_982 (Section 8. Digital economy).