

(English version)

**Question for written answer E-003060/25
to the Commission
Jorge Buxadé Villalba (PFE)
(23 July 2025)**

Subject: Risks to European security posed by the contract between Pedro Sánchez's Government and the Chinese company Huawei

The Spanish Government has contracted Huawei, which has links with China's intelligence apparatus, to provide servers for storing court-authorised wiretaps from SITEL (Integrated Telecommunications Interception System). Many Western States consider Huawei to be a high-risk critical infrastructure supplier ⁽¹⁾.

Despite warnings from the Commission and other international allies, Spain's socialist Government has decided to ignore the security implications this could have for judicial and police cooperation both nationally and at European level.

This decision not only violates the principle of national security as part of a robust EU strategy, but also lays the Spanish judicial system's most sensitive data open to potential foreign interference. In addition, it goes against the objectives of the EU toolbox for 5G security and the NIS 2 Directive.

1. Does the Commission consider this contract to be in line with EU recommendations for 5G security and the implementation of the NIS 2 Directive?
2. Will the Commission assess the security risks posed by the fact that Spanish surveillance and court-authorised wiretapping systems are using Chinese hardware?
3. What action will the Commission take to ensure that Pedro Sánchez's unilateral decisions do not compromise EU security?

Submitted: 23.7.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(17 September 2025)**

In the communication on the implementation of the EU 5G cybersecurity toolbox of 15 June 2023 ⁽¹⁾, the Commission assessed that Huawei (and ZTE) present materially higher risks than other 5G suppliers and committed to avoid exposure of its own corporate communications networks to mobile networks using Huawei and ZTE as suppliers and to restrict these suppliers from relevant funding EU programmes and instruments.

The Commission also considered that decisions adopted by the Member States to restrict or exclude Huawei and ZTE are justified and compliant with the 5G Toolbox. It urged all Member States to implement the 5G Toolbox and take measures to mitigate the risks linked to these suppliers.

The contract concluded by the Spanish Ministry of the Interior with Huawei can potentially create a dependency on a high-risk supplier in a critical and sensitive sector that would increase the risk of foreign interference.

In line with the 5G Toolbox and as announced in the ProtectEU Strategy ⁽²⁾ of April 2025, the Commission will look more broadly at the security and resilience of information and communication technology (ICT) supply chains and infrastructure in the upcoming revision of the Cybersecurity Act, with a view to avoid critical dependencies and de-risk our ICT supply chains from high-risk suppliers.

¹ European Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States: <https://digital-strategy.ec.europa.eu/en/news/commission-announces-next-steps-cybersecurity-5g-networks-complement-latest-progress-report-member>

⁽¹⁾ C(2023) 4049.

⁽²⁾ COM(2025) 148.