

(English version)

Question for written answer E-003576/25
to the Commission
Tobiasz Bocheński (ECR)
(17 September 2025)

Subject: Risk associated with importing electronic devices from China that may allow unauthorised access to data

More and more Member States and EU companies are expressing serious concern over the trustworthiness and security of electronic components imported from China. In recent years, there have been many reported instances of devices from China that were found to contain hidden chips or components that were not included in the technical specification provided by the manufacturer or contract documentation.

For example, Supermicro servers, used by providers of cloud services and public institutions, among others, were found to contain microscopic integrated circuits that could enable remote access to data. In recent years, similar incidents have also been reported in connection with closed-circuit cameras, 5G modems, routers and IoT devices imported from China. These constant and systematic reports come at a scale that may threaten the EU's digital security and strategic independence.

1. Are there measures planned to increase the monitoring of supply chains in the information and communications technology (ICT) sector, including mandatory security audits of electronic products used in the public administration, critical infrastructure and strategic sectors?
2. Is the Commission considering introducing a European security certification mechanism for electronic equipment, similar to the standards applied in the defence and energy sectors, to limit reliance on non-EU suppliers whose activities do not conform to transparency and trustworthiness standards?

Submitted: 17.9.2025

Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(31 October 2025)

High dependency on non-European suppliers, in particular high-risk suppliers, can lead to increased information and communication technology (ICT) supply chains security risks, including the possibility of foreign interference.

Cybersecurity certification established by Regulation 2019/881 of the European Parliament and of the Council (the Cybersecurity Act) ⁽¹⁾ is essential for enhancing resilience and trust in the Single Market.

It provides for expert evaluation and offers evidence to customers that ICT products, services, processes and managed security services comply with specified functional security requirements.

The NIS2 Directive ⁽²⁾ places legal duties on 'essential' and 'important' entities to manage supply-chain risks as part of their overall cybersecurity risk-management obligations (third-party risk assessments, contractual/technical controls, vulnerability handling, incident reporting, use of certified ICT where appropriate), while the Cyber Resilience Act ⁽³⁾ imposes product-level obligations on manufacturers/importers/distributors of 'products with digital elements' so that components and final products are designed, documented and maintained securely across the product life cycle (mandatory software bill of materials, vulnerability-handling, security updates, documentation and conformity/market surveillance).

As announced in the ProtectEU Strategy ⁽⁴⁾ of April 2025, the Commission will look more broadly at the security and resilience of 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⁾ Regulation (EU) 2019/881.

⁽²⁾ Directive (EU) 2022/2555.

⁽³⁾ Regulation (EU) 2024/2847.

⁽⁴⁾ COM(2025) 148.