

(English version)

**Priority question for written answer P-003323/25
to the Commission
Tomáš Zdechovský (PPE)
(28 August 2025)**

Subject: Security risks posed by the use of Chinese-manufactured drones by EU security and enforcement bodies

Recent analyses, including studies by Ruhr University Bochum and the Center for IT Security, Privacy and Accountability, as well as national warnings, have identified serious technical vulnerabilities in Chinese-manufactured unmanned aerial systems (notably those made by Da-Jiang Innovations), including risks of data exfiltration, telemetry misuse, and potential supplier leverage by a hostile state. Some Member States (e.g., Lithuania and the Netherlands) have already restricted the use of these systems in defence and public security sectors. EU frameworks such as the NIS2 Directive ⁽¹⁾ and the Cyber Resilience Act ⁽²⁾ provide tools to manage supplier risk and ensure data integrity.

1. Is the Commission aware of the security implications of the continued use of Chinese drones by enforcement and emergency services in the EU, and what assessment has been made regarding the associated data security and supplier-dependence risks?

2. Does the Commission intend to propose measures — such as procurement guidelines, mandatory EU cybersecurity certification for drones, or a temporary moratorium on high-risk suppliers — to ensure that drones deployed in sensitive sectors cannot transmit data outside the EU or store it in non-EU countries?

Submitted: 28.8.2025

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

Unmanned aircraft systems (UAS) and their rapidly advancing capabilities pose a growing security and cybersecurity risk, for example if being used for digital reconnaissance.

The Cyber Resilience Act (CRA) ⁽¹⁾ provides for mandatory cybersecurity requirements for the design, development and production of products with digital elements. UAS, as products with digital elements, would be covered by these new rules, with the exception of those developed exclusively for national security or military purposes.

The CRA also does not apply to products in the area of aviation, including UAS, that have been certified in accordance with Regulation (EU) 2018/1139 ⁽²⁾.

In addition, Article 22 of the directive (EU) 2022/2555 ⁽³⁾ establishes a legal basis to carry out coordinated security risk assessments of specific critical information and communication technology (ICT) services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors ⁽⁴⁾.

As announced in the ProtectEU Strategy ⁽⁵⁾ of April 2025, the Commission is currently looking more broadly at the security and resilience of ICT supply chains and infrastructure in the upcoming revision of the Cybersecurity Act ⁽⁶⁾, with a view to avoid critical dependencies and de-risk our ICT supply chains from high-risk suppliers.

As set in the EU Drone Strategy 2.0, the Commission will define criteria and labelling schema for a voluntary 'European Trusted Drone' label.

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, 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, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

² Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

⁽¹⁾ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance) <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.

⁽²⁾ Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.) <https://eur-lex.europa.eu/eli/reg/2018/1139/oj/eng>.

⁽³⁾ <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.

⁽⁴⁾ Such risk assessments are to be conducted by the Network and Information Systems (NIS) Cooperation Group, in cooperation with the Commission and ENISA.

⁽⁵⁾ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0148>.

⁽⁶⁾ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>.

This label would be granted to drones that demonstrate secure design, encrypted communications, and protection against malicious interference throughout their lifecycle. This work is supported by the European Parliament Pilot Project.
