

**Priority question for written answer P-003323/2025
to the Commission**
Rule 144
Tomáš Zdechovský (PPE)

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 Directive¹ and the Cyber Resilience Act² 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

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>).