

(English version)

**Question for written answer E-000481/26
to the Commission**

**Hélder Sousa Silva (PPE), Lúcia Pereira (PPE), Paulo Cunha (PPE), Sebastião Bugalho (PPE), Wouter Beke (PPE),
Pekka Toveri (PPE), Alice Teodorescu Măwe (PPE)**

(6 February 2026)

Subject: Russian proximity operations and EU satellite communications security

Reports indicate that Russian ‘Luch’ vehicles have conducted repeated close-proximity manoeuvres near European geostationary satellites and may have intercepted communications, including potentially vulnerable command-and-control links on older systems. In the context of the EU Space Strategy for Security and Defence, the implementation of the European Union Governmental Satellite Communications (GOVSATCOM) and the roll-out of the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) system, this raises urgent questions about resilience, accreditation and user trust when it comes to EU satellite communications.

1. What is the Commission’s current assessment, including through relevant EU bodies and Member States, of the exposure of satellites serving Europe to interception of uplinks and to capture/replay of command links, and what immediate mitigation measures (technical and operational) is it promoting in 2026?
2. What mandatory security requirements will the Commission impose, via accreditation and procurement, on EU-funded or EU-supported future systems intended to serve security and defence needs (including GOVSATCOM/IRIS²), notably end-to-end encryption for telemetry, tracking, and command, strong authentication, secure key management and resilience against jamming/spoofing of satellites?
3. What concrete framework will the Commission put in place to ensure that Ministries of Defence and commercial users can trust EU space infrastructure, including auditable certification, supply-chain security requirements and continuity-of-service plans?

Submitted: 6.2.2026

**Question for written answer E-000524/26
to the Commission**

Sofie Eriksson (S&D), Bruno Tobback (S&D), Bruno Gonçalves (S&D), Eero Heinäluoma (S&D), Nicola Zingaretti (S&D), Jens Geier (S&D), Giorgio Gori (S&D)

(9 February 2026)

Subject: Russian space activity exposes vulnerabilities in Europe’s satellite infrastructure

The European security environment has changed significantly in recent years. Russia’s full-scale invasion of Ukraine has demonstrated that hybrid threats and intelligence activities are now central elements of the security landscape. These threats increasingly extend beyond land, air and sea and into space.

Recent reporting by the *Financial Times* indicates that European security and intelligence sources believe that Russian space vehicles have conducted close manoeuvres near European geostationary satellites, highlighting vulnerabilities in Europe’s satellite infrastructure.

Particular concern has been raised regarding older European satellites that lack modern encryption and advanced onboard security features.

EU space infrastructure underpins a wide range of critical functions, including communications, navigation, energy systems and crisis response. Disruption, interference or loss of control over these assets could therefore have serious consequences for European security, economic stability and societal resilience.

Against this background, we would like to ask whether the Commission has considered carrying out, or has already carried out, a comprehensive vulnerability assessment of the EU’s space infrastructure? If not, does the Commission intend to initiate such an assessment as part of its work on EU security and resilience?

Submitted: 9.2.2026

Joint answer given by Mr Kubilius on behalf of the European Commission
(27 April 2026)

Pursuant to Articles 34(2) of the Space Programme Regulation ⁽¹⁾ and 30(3) of the Secure Connectivity Regulation ⁽²⁾, the Commission determines General Security Requirements (GSR) for all its space systems to address current and future threats upon them, such as replay and jamming/spoofing attacks.

The GSR are EU classified information and are based on a security risk assessment which systematically analyses relevant risks considering the geopolitical context and the capabilities of state actors.

The Commission relies on the Security Accreditation Board (SAB), an independent body composed of EU Member State representatives, established by Article 36 of the Space Programme Regulation, to provide security accreditation of EU space infrastructures before their deployment and operations by auditing all components and procedures to ensure full respect of the security requirements contained in the respective GSR.

Moreover, risks linked to the supply chain of EU space systems are limited through eligibility and participation conditions defined in Article 24 of the Space Programme Regulation and Article 22 of the Secure Connectivity Regulation.

Consequently, thanks to their security design, even if some of the targeted satellites host payloads for the EU space programme no effect is identified. European commercial sector satellites may be more exposed to interference or malicious activities.

Therefore, the Commission proposal for an EU Space Act ⁽³⁾ in June 2025 aims to enhance the resilience of commercial and governmental satellites.

Furthermore, the Council Decision on the security of systems and services deployed, operated and used under the Space Programme ⁽⁴⁾ lays down operational provisions to respond to threats upon need.

⁽¹⁾ OJ L 170, 12.5.2021, pp. 69-148, ELI: <http://data.europa.eu/eli/reg/2021/696/oj>.

⁽²⁾ OJ L 79, 17.3.2023, pp. 1-39, ELI: <http://data.europa.eu/eli/reg/2023/588/oj>.

⁽³⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0335>.

⁽⁴⁾ OJ L 170, 12.5.2021, pp. 178-182, ELI: <https://eur-lex.europa.eu/eli/dec/2021/698/oj/eng>.