

Question for written answer E-000481/2026

to the Commission

Rule 144

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

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