Council of the European Union

Brussels, 3 December 2025
(OR. en)

15986/25

TELECOM 434
TRANS 591

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	AOB for the meeting of the Transport, Telecommunications and Energy Council on 5 December 2025: Global Navigation Satellite Systems (GNSS) jamming and spoofing : Towards Enhanced Security and Protection - Information from Czechia, Estonia, Finland, Germany, Latvia, Lithuania, Poland, Slovenia, Slovakia and Spain

Non-paper from Czechia, Estonia, Finland, Germany, Latvia, Lithuania, Poland, Slovakia, Slovenia, and Spain

Global Navigation Satellite Systems (GNSS) jamming and spoofing: Towards Enhanced Security and Protection

GNSS interference—both jamming and spoofing—is emerging as a significant and steadily growing security concern for Europe. While the EU and its Member States are taking steps to address it, these efforts have not been enough to reverse the trend. What started as a risk mainly to aviation has now spread to maritime and land transport, mobile networks, public-safety communications, and even radio and TV broadcasting. The interference is becoming more frequent and more sophisticated, disrupting the reliable operation of services on critical infrastructure and causing growing economic damage across the region. Several studies have assessed the impact of GNSS on EU GDP to be above 10%.[1]

The roundtable discussion, convened by Lithuania on 13 November 2025, provided an opportunity for a wide range of stakeholders to exchange best practices and showcase private-sector

[1] DG DEFIS briefing on GNSS Interference, SWP 11 Nov 2025

contributions to strengthening resilience against this hybrid threat. Compared to the March 2025 event organized by Lithuania on the same issue, the situation has evolved.

According to available data from the Communications Regulatory Authority of the Republic of Lithuania, the number of detected interference sources in the Kaliningrad region increased from 5 in March 2025 to 31 by October 2025. A similar tendency is occurring in the Leningrad region according to Communications Regulatory Authority of the Republic of Estonia. These developments suggest the presence of a structured and centrally managed capability that could enable jamming or spoofing activities at varying levels of intensity if activated. Such an infrastructure would, in principle, allow for disruption across multiple radio-frequency bands, even if not all of them are currently being affected. This is happening even though the International Telecommunications Union's Radio Regulations Board (ITU RRB) in its decision "*again urged the Administration of the Russian Federation to take all possible actions to immediately cease any source of harmful interference to safety services in the RNSS"*.[2]

Private-sector representatives highlight several priority needs, including more proactive and coordinated action, investment in alternative navigation solutions, the development of a centralized system, fiber-based time synchronization. They also underscore the importance of tangible support for innovation in anti-jamming and anti-spoofing technologies. In addition, the maritime sector points to the absence of operational guidance on addressing jamming and spoofing incidents, including possibility to share interference data from the maritime domain in a centralized manner.

Conclusions and recommendations

While the situation has evolved, the call of the seventeen ministers to the Commission to take actions regarding the GNSS interference, together with a proposal for a 12-point action plan (6 June 2025) remains highly relevant. Development of action plans for different domains (space, aviation, maritime, telecommunications) to avoid potential duplication of efforts and coordination of short-term and long-term measures at EU and national level are of utmost importance, as evidenced by the following:

- The EU response to jamming and spoofing remains largely focused on individual defensive measures, even though harmful interference has persisted for several years and continues to intensify.
- Permanent, centrally controlled infrastructure for jamming and spoofing purposes, was built by russia in Kaliningrad region during 2025. This activity violates international obligations and agreements and poses threat to our critical infrastructure.
- Lack of international law enforcement tools is clear: most affected EU Member States continue documenting violations and raising the issue in forums such as the ITU Radio Regulations Board and the World Radiocommunication Conference, International Civil Aviation Organization, etc. However, these mechanisms cannot ensure compliance or

[2] Document RRB25-3/33-E, 14 November 2025

deterrence: when a country does not cooperate, the dispute-resolution process stalls. This situation underscores the need to update international rules accordingly.

- GNSS interference monitoring and early-warning systems are being deployed across different sectors and Member States, but a merely decentralized approach leads to fragmentation. Establishing a single EU-level focal point with a centralized reporting and data-sharing platform, based on voluntary national monitoring and aggregating non-classified information on observed RFI, would improve coordination and ensure access to consistent and reliable information.
- At least two alternative, independent solutions should be implemented and/or maintained across different domains to ensure safe navigation. Achieving this will require investment beyond standard operational practice.
- The private sector has called for urgent support to accelerate the development and deployment of anti-jamming and anti-spoofing technologies and called for more proactive and coordinated action, including the development of a centralized monitoring and early-warning system.

Call for action:

We continue to call for the adoption of a comprehensive and coordinated action plan to address GNSS interference, incorporating short-, medium-, and long-term measures across all relevant sectors. An EU-level approach integrating diplomacy, legal measures, and technological resilience is essential, as the only way that can effectively address systemic and cross-border hybrid threats.