Council of the European Union

Brussels, 22 May 2025
(OR. en)

9198/25

TELECOM 150
ESPACE 38
TRANS 194

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	AOB for the meeting of the Transport, Telecommunications and Energy Council on 6 June 2025: Call for common actions in response to Global Satellite Navigation Systems (GNSS) jamming and spoofing threats - Information from Lithuania, Denmark, Estonia, Finland, Germany, Latvia, Slovenia and Spain

Global Satellite Navigation Systems (GNSS) provide positioning, navigation, and timing services, which are vital to ensure safe operation of aviation, maritime, and other means of transport. Timing services of the GNSS also serve for time synchronization of telecommunication networks, and, thus, are vital to enable seamless communication, synchronize financial transactions, stabilize power grids, etc. In many regions, including Europe, GNSS is mostly based on Global Positioning System (GPS), but also on Galileo is widely used service for real-time determination of positioning. However, these systems are increasingly under threat that is not likely to stop in the near future.

Starting 2022, two types of interference to GNSS - jamming[1] and spoofing[2] - have been observed in the airspace of the Baltic Sea Region, originating mainly from the sources in Russia and Belarus. Since August 2024, a dramatic increase in jamming and spoofing of GNSS signals for aircrafts has been recorded[3]. Since the beginning of 2025, interference to GNSS receiving signals in sea vessels has also been observed more frequently. Disruptions to these systems have far-reaching consequences.

---

1 *Jamming - type of* deliberate radio interference via electronic warfare systems when information about an aircraft location, altitude, and time is not received.

2 *Spoofing* - type of deliberate radio interference when an electronic warfare systems send wrong GPS signals and aircraft location, altitude, and time are displayed incorrectly, e.g. an aircraft is shown to be in a different location than it really is.

3 In Lithuania: starting from 556 cases in March 2024 to 890 in October 2024 and 1185 in January 2025; in Latvia: from 790 cases in October 2024 to 1288 cases in January 2025; in Estonia: 1150 cases in October 2024 and 1085 cases in January 2025; in Poland: 1908 cases in October 2024 to 2732 cases in January 2025 (according to unique ICAO ID per month).

GNSS interference cases are not random incidents but a systematic, deliberate action by Russia and Belarus, which can be used as a hybrid attack on strategic radio spectrum, which is essential for modern technology and regional safety and security. So far, causing significant damage has been simple and cheap, without taking any responsibility. Therefore, this activity is most likely to continue unless proportional counter measures are taken.

GNSS interference as a growing safety and security concern requires immediate coordinated action. So far, the attempts by several Member States to address the problem have not brought any more tangible results. Therefore, it is necessary to increase diplomatic efforts to address the interference and put the pressure on the responsible parties. At the same time, the development of technical solutions to reduce vulnerabilities and strengthen the resilience of GNSS must be accelerated, taking into account that transport, energy, telecommunications and financial sectors are also dependent on reliable GNSS services.

We call for the actions outlined in the Ministers' letter, which will be signed by several Member States during the TTE Council meetings on 5-6 June. The letter is addressed to the High Representative Ms. Kaja Kallas, the Executive Vice-President Ms. Henna Virkkunen, the Commissioners Mr. Andrius Kubilius, Mr. Apostolos Tzitzikostas, and Mr. Piotr Serafin.

Among others, these actions are most relevant to the Telecommunications and Digital Ministers:

1. Evaluate and coordinate the possibility to **suspend the right to Russia and Belarus in the ITU** to register the use of radio resources while GNSS interference is in progress. The lack of procedural legislation cannot be an excuse for deliberately contravening the spirit of the ITU Constitution and its general principles, endangering public health and life, without suffering any consequences.
2. Based on good practice of EU and NATO cooperation on critical undersea infrastructure, **enhance civil-military coordination** mechanisms among Member States for shared monitoring, data exchange, and possible response to GNSS interference. Explore the benefits of dual use of various equipment and measures to combat the risks caused by GNSS interference.
3. **Intensify RFI monitoring** by eligible national organizations and bodies, e. g. national regulator, police and military, and aggregate non-classified information on observed RFI to a publicly available near real-time monitoring and alert service on European level.
4. Accelerate the **deployment of interference resistant GNSS services**, especially the anti-spoofing features that are part of the Galileo program, e. g. authentication and/or encryption of signals exchanged between stations and user equipment.
5. Reassess the current reliance on GNSS-based navigation and **develop resilient Positioning, Navigation and Timing (PST) services** by deploying alternative or complementary systems, including ground-based legacy solutions. Simultaneously, upgrade and **modernize conventional navigation infrastructures** to serve as robust backups.
6. **Promote industry-manufacturer collaboration** for mitigation tools and updates. Support operator-level reviews of backup system readiness, ensuring non-GNSS alternatives are usable and practiced.

7. Draw the attention of critical infrastructure operators and unmanned system manufacturers to the risks that may arise from interference with GNSS.
8. **Develop action plans** for different domains (space, aviation, maritime, telecommunications) to avoid potential duplication of efforts and coordinate short-term and long-term measures at EU and national level.
9. **Continue cooperation** with all relevant stakeholders (ITU, ICAO, IMO, EASA, EMSA, IATA, EUROCONTROL).

These actions, among others, could contribute to building the overall resilience of the critical infrastructure and strengthening safety and security in Europe.