

Rising GNSS Spoofing Threat: Why Delhi's Airspace Faced Navigation Disruptions

November 16, 2025 • vajiramandravi.com



GNSS Spoofing Latest News

- In early November, several aircraft flying over Delhi experienced GNSS (Global Navigation Satellite System) spoofing, where satellite navigation signals were manipulated without warning. Such incidents are uncommon outside border or conflict areas.
 - GNSS is a general term for satellite-based systems that provide positioning, navigation, and timing (PNT) services on a global scale.
 - E.g., – Russia's GLONASS, Europe's Galileo, China's BeiDou etc.
- Following the disruption, the government ordered an investigation led by the **National Security Council Secretariat (NSCS)** under National Security Adviser Ajit Doval.

GNSS Spoofing Near Delhi: A New and Unusual Safety Threat

- Aircraft flying near Delhi recently faced **GNSS spoofing**, where fake satellite signals give wrong navigation data. Pilots reported incorrect aircraft positions and false terrain warnings.
 - An Air India pilot said he faced spoofing on all six days he flew in early November. These signals were detected within **60 nautical miles of Delhi**.
- Because navigation systems became unreliable, air traffic controllers had to give **manual guidance** to pilots.
- GNSS spoofing is usually seen only in **war zones or border areas**, such as West Asia, eastern Russia, and India's borders with Pakistan and Myanmar.
- It had **never been reported before over a major inland city** like Delhi. It should be noted that VIP movements do not cause spoofing; they only involve **GNSS jamming**, not false signals.
- No NOTAM (warning notice) was issued to explain the interference.
 - A NOTAM, or Notice to Airmen, is a notification issued by aviation authorities to alert pilots and other aviation personnel of potential hazards or changes that could affect flight safety.
- The National Security Council Secretariat under Ajit Doval has launched an investigation.

About GNSS Spoofing

- Modern aircraft depend heavily on **GNSS/GPS signals** for navigation, timing, terrain awareness, and communication.
- When these signals are faked or altered, aircraft systems may show:
 - Wrong positions
 - False terrain or runway warnings
 - Incorrect braking cues
 - Errors in communication and surveillance systems
- Spoofing usually doesn't immediately endanger a flight because aircraft have **backup systems**, like the Inertial Reference System, which works for up to five hours even if GPS fails.
- However, spoofing still affects safety by confusing pilots, creating false alerts, and increasing workload — especially when no NOTAMs warn them in advance.
- Even after the aircraft leaves the spoofed zone, some systems may **not reset properly** and may continue showing false alerts or navigation errors. This makes the situation harder to manage.

How Spoofing Became a Global Aviation Problem

- According to a 2024 OPS Group report:
 - GPS spoofing grew sharply after September 2023.
 - By January 2024, around 300 flights per day were affected.
 - By August 2024, spoofing hit 1,500 flights daily.
 - In one month (July 15–August 15, 2024), 41,000 flights worldwide experienced spoofing.
- The Delhi region ranked among the top 10 global hotspots, reporting 316 spoofing events during the same period.

India's Exposure to Spoofing Events

- Government data shows 465 GPS interference and spoofing incidents in India's border areas — mainly Amritsar and Jammu — between November 2023 and February 2025, roughly one event per day.
- Delhi saw several spoofing events despite being far from conflict zones.

Actors Behind GPS Spoofing

- Primary actors include:
 - Military units using spoofing to mislead enemy drones and GPS-guided weapons in conflict zones.
 - There are also claims of deliberate targeting of civilian aircraft, particularly in regions around Russia.

Global Aviation Leaders Call for Stronger Protection

- Experts urged all nations and agencies to protect civilian flights and airports, reminding that international law bans targeting civil aviation.
- They stressed the need for urgent global action against spoofing and jamming threats.

IATA's Multi-Layered Strategy to Tackle GNSS Spoofing

- At the ICAO Assembly, IATA proposed a comprehensive plan to address the growing risk of spoofing:
 - Standardised reporting for all GNSS interference events
 - Stronger cross-border cooperation and real-time information sharing
 - Regulation and enforcement on the sale and use of jamming devices
 - Better spectrum management at national and global levels
 - Advanced detection systems to identify interference early
 - More resilient GNSS receivers, with anti-jamming and anti-spoofing technology built into aircraft systems.
- These steps aim to build a global shield against spoofing and protect aviation safety.

Why India Needs Faster Response and Transparency

- Repeated spoofing incidents around Delhi, Mumbai, and Kolkata have raised serious safety concerns in India.
- Delayed communication and limited transparency make it difficult for airlines and pilots to take timely decisions.
- This undermines trust among flight crews and passengers and highlights the urgent need for clear reporting protocols, faster alerts, and stronger technical safeguards.

Source: TH | TI | IT

Source: <https://vajiramandravi.com/current-affairs/rising-gnss-spoofing-threat-why-delhis-airspace-faced-navigation-disruptions/>

© Vajiram & Ravi. For personal use only.