

7. Global Navigation Satellite System – Science & Technology

Aircraft flying over Delhi recently faced a critical threat from GNSS spoofing, where fake satellite signals are broadcast to mislead navigation, unlike jamming which merely blocks signals. This poses a severe security risk to civil aviation, demonstrated by a rapid global rise in such military-attributed interference events in hotspots like the Delhi region.

Understanding GNSS and Spoofing

Global Navigation Satellite System (GNSS)

Definition – GNSS refers to a constellation of satellites that provide essential positioning, navigation, and timing (PNT) services globally.

Function – It uses signals from multiple satellites to determine a user's exact location, velocity, and time anywhere on Earth.

Major Systems – Includes GPS (USA), GLONASS (Russia), Galileo (EU), BeiDou (China), and regional systems like NavIC (India) and QZSS (Japan).

Aviation Reliance – Modern aircraft rely heavily on GNSS for terrain awareness, collision avoidance, autopilot, and communication synchronization.

GNSS Spoofing

Definition – GNSS spoofing involves broadcasting fake satellite signals to mislead receivers into calculating incorrect location, speed, or time.

Core Concept – Spoofing is a deliberate attempt to falsify, forge, or manipulate digital data or signals so that a system or user believes it is coming from a trusted or legitimate source.

Purpose – It is used to steal sensitive information, redirect navigation, commit financial fraud, hijack communications, or bypass authentication.

How GNSS Spoofing Works

Spoofing is a subtle, technical attack designed to deceive the receiver –

Signal Generation – A spoofer generates counterfeit satellite signals using the same frequency and format as authentic GNSS transmissions.

Overpowering – Spoofed signals are transmitted at higher power than genuine satellite signals, causing the aircraft/device to automatically lock onto the stronger signal.

Gradual Deception – The spoofer slowly shifts the navigation data, position, altitude, or timing. Because the shift is subtle, aircraft systems often don't detect a sudden anomaly.

Result – The cockpit instruments display incorrect aircraft location or altitude as if they were real.

Spoofing vs. Jamming (Differentiation)

Feature	Jamming	Spoofing
Nature of Attack	Blocks or disrupts signals so that a receiver cannot obtain valid data.	Replaces or mimics signals to feed false information to the receiver.
Objective	Aims to deny service by overwhelming or interfering with signals.	Aims to deceive by making the receiver accept fake signals as real.
Effect on Device	Causes devices to lose connectivity or fail to function.	Causes devices to operate incorrectly based on false information.
Detection Difficulty	Easier to detect because the signal loss is immediate and obvious.	Harder to detect because the receiver still receives signals that appear normal.
Security Risk	Poses mainly operational disruption risks.	Can cause strategic risks (ship deviation, drone hijacking, military miscalculations).

Threats, Risks, and Global Trends

Threats and Safety Risk – Spoofing is a serious aviation threat because it targets the core PNT data –

False Location Data – Displays incorrect aircraft positions, endangering altitude and terrain awareness.

Alerts and Disruption – Triggers false terrain and obstacle warnings, increasing pilot workload, and affects surveillance systems and ATC communication links.

System Persistence – Faulty readings may not correct automatically, causing ongoing navigation errors even after leaving the spoofed zone.

Strategic Vulnerability – Can be used for hostile actions, affecting national security and civil-aviation safety. (Note – Modern aircraft have multiple backups, such as the Inertial Reference System (IRS), which can function independently of GNSS for up to five hours.)

Global Trends and Hotspots

GNSS spoofing severely impacted civil aviation beginning September 2023 –

Escalation – The average number of spoofed flights rose from 300 flights per day in January 2024 to 1,500 flights per day by August 2024.

Hotspots – Delhi region was among the top 10 spoofing hotspots globally, alongside locations in Cyprus, Israel, Egypt, Turkey, Russia, Pakistan, Belarus, and Lebanon.

Actors – Major spoofing activity is conducted by military units targeting hostile drones or missile systems, though some allegations point to malicious targeting of civilian aircraft.

Examples – The aircraft of EU President Ursula von der Leyen faced GNSS disruption over southern Bulgaria in September 2024, allegedly due to Russian interference. An Azerbaijan Airlines flight crashed in Kazakhstan in December 2024, reportedly linked to suspected spoofing.

Proposed Solutions – International and industry bodies are pushing for standardized mechanisms and resilient technology.

Global Safety Appeal (IATA) – Urged all parties to ensure the safety of civilian flights, stressing that international law prohibits targeting civil aircraft.

ICAO Recommendations – Proposed measures at its 42nd Assembly include –

1. Standardised reporting mechanisms and stronger cross-border cooperation.
2. National regulation on the sale and use of jamming/spoofing devices.
3. Deployment of advanced detection systems and better spectrum management.
4. Development of resilient anti-jamming and anti-spoofing GNSS receivers.

Industry Push – The aviation sector seeks proactive avionics upgrades, greater transparency in reporting, and real-time threat identification.

Source – [https://www.thehindu.com/sci-tech/technology/what-are-the-threats-from-gnss-spoofing-explained/article70284960.ece#-~-](https://www.thehindu.com/sci-tech/technology/what-are-the-threats-from-gnss-spoofing-explained/article70284960.ece#-~-text=The%20story%20so%20far%3A%20In%20border%20regions%20or%20conflict%20zones)

[text=The%20story%20so%20far%3A%20In%20border%20regions%20or%20conflict%20zones](https://www.thehindu.com/sci-tech/technology/what-are-the-threats-from-gnss-spoofing-explained/article70284960.ece#-~-text=The%20story%20so%20far%3A%20In%20border%20regions%20or%20conflict%20zones)