What are the threats from GNSS spoofing?

Why did pilots encounter manipulated Global Navigation Satellite System signals while flying over Delhi? Which institution is heading the inquiry? How do such occurrences endanger aircraft safety? What has the aviation industry been pushing for?

Jagriti Chandra

The story so far:

In early November, aircraft flying over Delhi encountered GNSS spoofing or manipulated Global Navigation Satellite System signals, catching pilots off guard as there had been no prior warning of such activity. Such interference is rare, barring at India's border regions or conflict zones. The government has since ordered an inquiry under the National Security Adviser Ajit Doval-headed National Security Council Secretariat (NSCS).

Is it a recent occurrence?

Aircraft flying over Delhi reported incidents of GNSS spoofing. These counterfeit signals cause erroneous navigation data in the cockpit, including incorrect aircraft positions and terrain warnings. An Air India pilot told *The Hindu* that he encountered spoofing on all six days he flew in and out of Delhi in the first week of November. Another pilot said his cockpit systems issued a false terrain warning, suggesting obstacles ahead where none existed. Other pilots encountered similar warnings while taking off from the airport. These events were being reported by aircraft within 60 nautical miles of Delhi. The disruption in navigational equipment often requires manual intervention, with controllers providing direct navigation guidance to cockpit crew. GNSS spoofing, or misleading satellite signals sent to trick air-borne receivers such as enemy drones, is increasingly used in modern warfare and is a growing menace for aircraft systems that rely on GNSS signals. It is a relatively recent phenomenon seen in conflict regions in West Asia, eastern Russia, and India's border with Pakistan and Myanmar since 2023. But such activity had not previously been documented over inland metropolitan airspace, barring sporadic instances of GNSS-jamming (blocking of GNSS signals) during VIP flight movements or Republic Day security protocols. However, this time no notice to airmen (NOTAM) were issued, warning of military exercises in Delhi that could explain why these signals were being encountered.

Officials have dismissed suggestions that VIP movements might have triggered the spoofing

Since the media reported the occurrences, the Directorate General of Civil Aviation (DGCA) issued a stricter Standard Operating Protocol (SOP) requiring pilots and air traffic controllers to report these events within 10 minutes of occurrence to enable agencies to swiftly recognise the source of false signals. The NSCS, headed by Mr. Doval, has set up a probe committee to investigate the matter. Officials have dismissed suggestions that VIP movements ahead of Bihar elections might have triggered these events, clarifying that security protocols during such operations involve GNSS jamming, not the transmission of false signals.

ISTOCKPHOTO

What is GPS spoofing?

Modern aircraft systems rely heavily on GNSS for accurate position, navigation, and timing. When these signals are tampered with, it can affect many systems, including terrain and runway warning systems, automatic braking, surveillance, and communication links between pilots and air traffic control. GNSS spoofing doesn't immediately hamper the safety of an aircraft, as aircraft systems are built with several redundancies, including the Inertial Reference System that's also used for navigation, which continue to operate safely for up to five hours even if a primary system fails. But such interference, whether intentional or accidental, can threaten safety by reducing pilot awareness, generating false alerts, and increasing their workload. The problem is harder to manage because affected areas are not always mentioned in NOTAMs, leaving crews unprepared.

According to a report by the OPS Group (a community of about 8,000 volunteers, including pilots, flight dispatchers, and air traffic controllers who exchange new information on risks to aviation safety) in 2024, GPS spoofing began to severely impact civil aviation in September 2023. In the first few months, relatively few aircraft were affected, but by January 2024, an average of 300 flights a day were being spoofed. By August 2024, this had grown to around 1,500 flights per day. An analysis by the OPS Group showed that for the one-month period from July 15-August 15, 2024, a total of 41,000 flights experienced spoofing. The report identified the Delhi region among the top 10 regions in the world that encountered large amount of spoofing after locations in Cyprus, Israel, Egypt, Turkey, Russia, Pakistan, Belarus, and Lebanon. According to government data, 465 GPS interference and spoofing incidents were reported in its border regions, primarily in the Amritsar and Jammu areas, between November 2023 and February 2025, which is an average of one event daily.

Primary actors currently carrying out GPS spoofing include military units targeting hostile drones in conflict zones or GPS-guided ammunition and missiles. But there have also been allegations of malicious attempts to target civilian aircraft, particularly against Russia.

What solutions have been proposed?

In September, the International Air Transport Aviation (IATA) presented a paper at the 42nd Assembly of the UN aviation safety watchdog International Civil Aviation Organisation in which it proposed a multi-faceted approach to respond to what it called "a persistent and growing risk to aviation safety". This includes developing a standardised reporting mechanism, strengthening cross-border cooperation and information-sharing, and enforcing national regulation concerning the sale, possession and use of jamming devices and more stringent national and international spectrum management. Other steps involve deployment of advanced detection systems, encouraging avionics manufacturers to proactively develop and deploy more resilient GNSS receivers with enhanced anti-jamming and anti-spoofing capabilities.