The Honourable Company of Air Pilots is the largest City of London Livery Company and the only one with a global membership. London Livery Companies are charitable specialist professional and trade bodies which, where relevant, seek to contribute their entirely independent and impartial expertise to their areas of interest. The Air Pilots Commercial Air Transport Team is directly supported by a large network of Company Members who review and validate our draft publications before issue.

If you would like to receive copies of new Safety Briefing Notes direct by email - or stop receiving them - please advise this to catcsg1@airpilots.org. All published Notes which continue to be relevant can be consulted at or downloaded from https://www.airpilots.org/CATSafetyBriefingNotes/.

AIR PILOTS - COMMERCIAL AIR TRANSPORT
SAFETY BRIEFING NOTE 18
[Issued 07 July 2025]

GNSS SIGNAL INTEGRITY

The Context
The extent of interference with the integrity of GNSS-based aircraft Position, Navigation and Timing (PNT) data has now increased beyond airport-specific issues preventing RNP approaches to become a significant en-route operational safety matter. It appears that risk exposure and the consequences of it are not dependent on which GNSS system is used - GPS is still the most used but Galileo, Beidou (China), GLONASS (Russia) and regional systems IRNS (India) and Japan (QZSS) are also in place.

Whilst it is not yet possible to illustrate this issue by including selected independently investigated events, we believe that a summary of the current risk and how to recognise and respond to it may be useful. It should be understood that whilst malicious GNSS signal disruption is area-specific, it may affect all aircraft or only intentionally-targeted ones. There appears to be no evidence to suggest that civil air traffic in general is an intentional target even though it is vulnerable when in areas where GNSS signal denial or interference is occurring. The origin and purpose of the disruption created is almost entirely military or paramilitary and therefore strongly linked to areas of local or regional conflict around the world. Typical targets for intentional GNSS signal disruption are airborne military assets and shipping in conflict areas with most sources of such interference on land and mobile. However, one recently destroyed disused oil rig being used for spoofing cargo ship navigation systems in the Black Sea had the unintended effect of disrupting aircraft in the area.

The Problem
Malicious interference with GNSS signals is now frequent in some parts of the world. Jamming (denial of a signal) and Spoofing (active interference with a signal) have different potential consequences. All GNSS satellite signals are easily overwhelmed by a terrestrial-source signal because it is much nearer to the aircraft and therefore much stronger. For both types of disruption, how long it will continue and the reliability of affected equipment once such disruption has ceased will be unknown. Detection of jamming or spoofing of an affected aircraft is currently limited to recognition of sudden changes to or loss of position data and/or GNSS signal strength. Improvements to GPS satellite resilience (although not to the other GNSS systems) are ongoing but are targeting a medium term resolution at best.

<u>Jamming</u>
This is intentional GNSS signal interference in a way that prevents airborne navigation equipment - including linked timing devices - from reliably locking on to signals from their source satellites. This will either completely block the signal or degrade it. The consequences will vary depending on the source satellite system and the dependent on-board equipment affected. If an on board navigation system can detect that it is being jammed, it may be able to automatically change to an alternative system and maintain normal function but if not, the aircraft position displayed will remain as it was when jammed.

<u>Spoofing</u>
This is the deliberate manipulation of genuine GNSS signals to distort their position or time information so that the on-board equipment feeds corrupted data to any aircraft system which uses these signals. This may include Hybrid INS, the aircraft clock, the weather radar, ADS-B and CPDLC. It may no longer be possible to reliably navigate as cleared or maintain situational awareness of other traffic in the vicinity and the ability of ATC to support safe traffic separation may be compromised technically or due to overload. However, if an INS is available and disconnected from the FMS prior to spoofing, it will

continue to provide broadly correct navigational guidance but without the usual GNSS updating, accuracy may decrease over time. EGPWS and other equipment which relies on GNSS input is unlikely to function reliably and, importantly, may remain unreliable after spoofing has ceased. Spoofing increases the risk of losing safe en-route separation and thereby increases mid air collision risk whilst occurring. RNP en-route navigation after spoofing may remain unreliable and RNP approaches should be explicitly avoided in these circumstances. False EGPWS hard warnings are also quite likely to occur.

The Current Geographic Risk Areas

Although GNSS signal disruption can occur anywhere, the areas currently most affected appear to be:

- Over and around the western Black Sea
- The eastern Mediterranean Sea and adjacent land areas
- The Baltic Sea and land areas around Kaliningrad
- Western Russia and Western Ukraine
- The Arctic Sea north of Finland and Northern Norway
- The India/Pakistan border area

The scale of the problem within many of the affected areas has continued to be significant. A review of recorded spoofing occurrences found that in a 30 day period in midsummer last year, over half of events for which an onset location was recorded occurred within the Nicosia, Cairo or Tel Aviv FIRs with the rest being distributed amongst 17 other FIRs. It also stated that in the same period, 41,000 spoofing events were reported, albeit highly concentrated in a very small proportion of global airspace.

Safety Recommendations

<u>To Aircraft Operators</u>

- Ensure pilots are aware of which aircraft equipment is vulnerable to GNSS signal interference and proactively provide appropriate simulator and/or ground training to ensure that they know how to recognise and respond to it and its aftermath in order to safely complete an affected flight.
- Consider procedures for proactively switching off GNSS before entering any known spoofing areas on the basis of time or distance to go and warn crews that jamming often precedes spoofing.
- Consider requiring that an information entry is made in the aircraft Technical Log at the end of any flight where GNSS signal disruption was detected which details the position disruption occurred and any observed consequences including any navigation system errors which continued after it.
- Consider restricting the use of either aircraft type or flight crew operating in known areas of the most frequent interference so that those pilots can be specially briefed and relevant aircraft maintenance personnel advised how to deal with post-flight Technical Log entries recording signal disruption.
- Review all aircraft equipment which relies on GNSS signal input with the respective manufacturers in order to understand any significant differences in aircraft vulnerability, pilot response procedures (e.g. if there are consequences when turning off the GNSS) and in post flight maintenance action.
- Consider including a record of the part numbers of potentially affected components in aircraft documents carried on board potentially vulnerable aircraft so that ATC can be advised if this aspect may be relevant to the wider management of a significant signal disruption event.
- Ensure that any suspected jamming or spoofing event is promptly reported to the relevant aviation safety regulator and that any specifically requested detail is provided.
- Examine the extent to which Flight Data Monitoring can detect exposure to GNSS signal disruption.

<u>To Pilots</u>

- If there is any heightened risk of GNSS signal disruption ensure that you have had a thorough pre-flight brief on the potential location, recognition and response to such a situation and are confident that you have enough information to respond to less accurate tracking. Also ensure your relevant systems knowledge relates specifically to the aircraft type you are operating and be aware of which en-route or potential diversion airports have non-GNSS approach procedures available. Availability of an analogue time source is recommended to guarantee that fuel endurance can be monitored.
- Inform ATC as soon as you detect any signal disruption, advise your OCC and make a Technical Log entry after flight so maintenance are aware and can carry out relevant checks.
- If GNSS jamming is suspected and non-hybrid INS reversion is available, continued navigation with reduced accuracy is possible but some dependent systems will retain errors for the rest of the flight.
- If GNSS spoofing occurs, navigation using it is not recommended and since incorrect height/altitude data will also affect EGPWS terrain proximity warning reliability, this system should be switched off.
- GNSS signal loss in airspace where ADS-B is required requires prompt advice to ATC.
- Document any events - position, apparent consequences and in-flight response - whilst these facts are still remembered and file this on the company safety reporting system as soon as practicable.