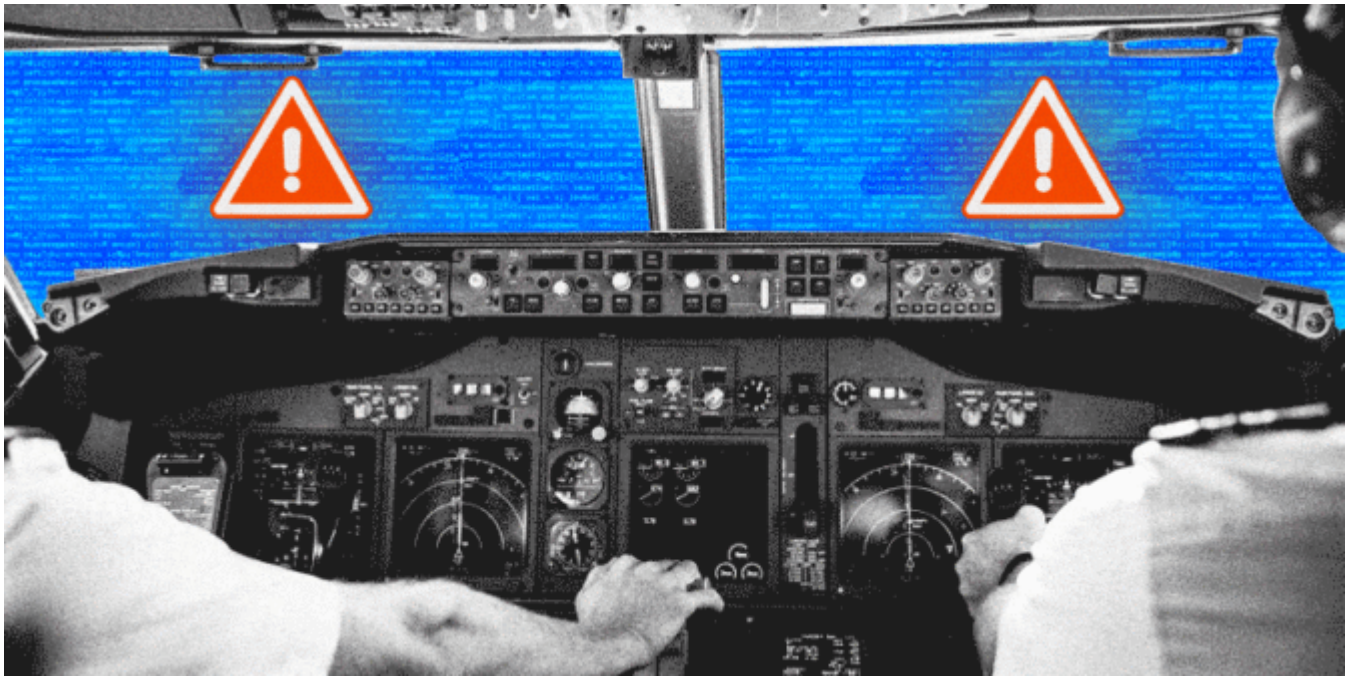
# Spoofed Before the NAT? Here's What to Do

Chris Shieff
21 October, 2025



An OPSGROUP member on a recent westbound NAT flight from the Middle East received the following message via CPDLC:


The crew contacted Shanwick via HF, who requested their **RNP capability** and operational status.

The controller explained that due to their point of departure (OMAA/Abu Dhabi) they wanted to be certain the aircraft had not been **contaminated by GPS jamming or spoofing** before it entered oceanic airspace.

It's been a while since we wrote about this procedure, and since then we've had this NAT Ops Bulletin published by ICAO telling operators what to do on the NAT if they've experienced jamming/spoofing, so we reached out to NATS directly for an update. **Here's what they had to say…**

## Defensive Measures

NATS reported they continue to receive a large number of flights every day that have been impacted by GPS interference prior to oceanic boundaries.

The issue is that once an aircraft's navigation system has been 'contaminated' by bad GPS data, it may not be possible to recover full RNP capability in flight, even if the normal GPS signal is restored.

These aircraft may no longer meet RNP 4/10 accuracy required in the NAT HLA, even **long after the trigger event occurred.**

The NAT Ops Bulletin which was published back in Jan 2025 requires crew of NAT-bound aircraft that have encountered GPS interference to notify their first NAT ANSP via RCL. Even if your aircraft shows no lingering effects, **ATC still want to know.**

NATS advise that late notification by pilots of a RNP degradation (such as approaching an oceanic entry point) greatly **increases controller workload.** They often need to move other aircraft out of the way to provide increased separation (in some cases from 14nm to 10 minutes), it's a big deal.

As a result, they are employing **defensive controlling measures.** Based on previously spoofed/jammed flights and regions of known risks, they may proactively contact flights assessed as higher risk to confirm status before entry – although the exact selection criteria isn't public. Increased separation will be applied until normal navigation performance is confirmed by the pilots.

In a nutshell, this is why the OPSGROUP member received the message above.

A special thank you to NATS for their help in answering this question.

## Jammed or spoofed? You need to let your NAT ANSP know

The NAT Ops Bulletin we keep mentioning – this provides the guidance for NAT traffic on how to manage GNSS interference. Here it is again, so you can't miss it! ⬇

NAT OPS BULLETIN

Serial Number: 2025_001 **Issued: 7 January 2025**
Subject: NAT GNSS Interference Procedures **Effective: 7 January 2025**
Originator: NAT SPG

The purpose of North Atlantic Operations Bulletin 2025-001 is to provide background information and guidance to aircraft operators in the North Atlantic (NAT) on the requirement to notify ATC of GNSS interference, and the Air Navigation Service Provider (ANSP) procedures that will be applied to aircraft that have been exposed to Global Navigation Satellite Systems (GNSS) interference (GNSS jamming and/or spoofing) during their flight.

***Any queries about the content of the attached document should be addressed to:***
*ICAO EUR/NAT Office: icaoeurnat@icao.int*

**NOTICE**
*NAT Ops Bulletins are used to distribute information on behalf of the North Atlantic Systems Planning Group (NAT SPG). The material contained therein may be developed within the working structure of the NAT SPG or be third party documents posted at the request of a NAT SPG Member State. A printed or electronic copy of this Bulletin, plus any associated documentation, is provided to the recipient as is and without any warranties as to its description, condition, quality, fitness for purpose or functionality and for use by the recipient solely for guidance only. The information published by ICAO in this document is made available without warranty of any kind; the Organization accepts no responsibility or liability whether direct or indirect, as to the currency, accuracy or quality of the information, nor for any consequence of its use. The designations and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.*

*The NAT OPS Bulletin Checklist is available at www.icao.int/EURNAT/EUR & NAT Documents, NAT Documents, then NAT Ops Bulletins.*

There is no objection to the reproduction of extracts of information contained in this Bulletin if the source is acknowledged.

NAT OPS Bulletin 2025_001_GNSS_RFI.docx Issued date: 07 January 2025

**Key takeaway from this: If you suspect or know that your aircraft has encountered any kind of GPS interference (both jamming or spoofing), NAT-bound traffic must let their first NAT ANSP know in the RCL – even if the aircraft appears to have recovered.**

This is prefixed by ‘ATC REMARKS/GNSS INTERFERENCE’ and must include details of any system degradations.

A few messages to keep handy are:

**‘ATC REMARKS/GNSS INTERFERENCE NO IMPACT.’**

**‘ATC REMARKS/GNSS INTERFERENCE NO CPDLC/ADS’**

**‘ATC REMARKS/GNSS INTERFERENCE RNP 10 ONLY’**

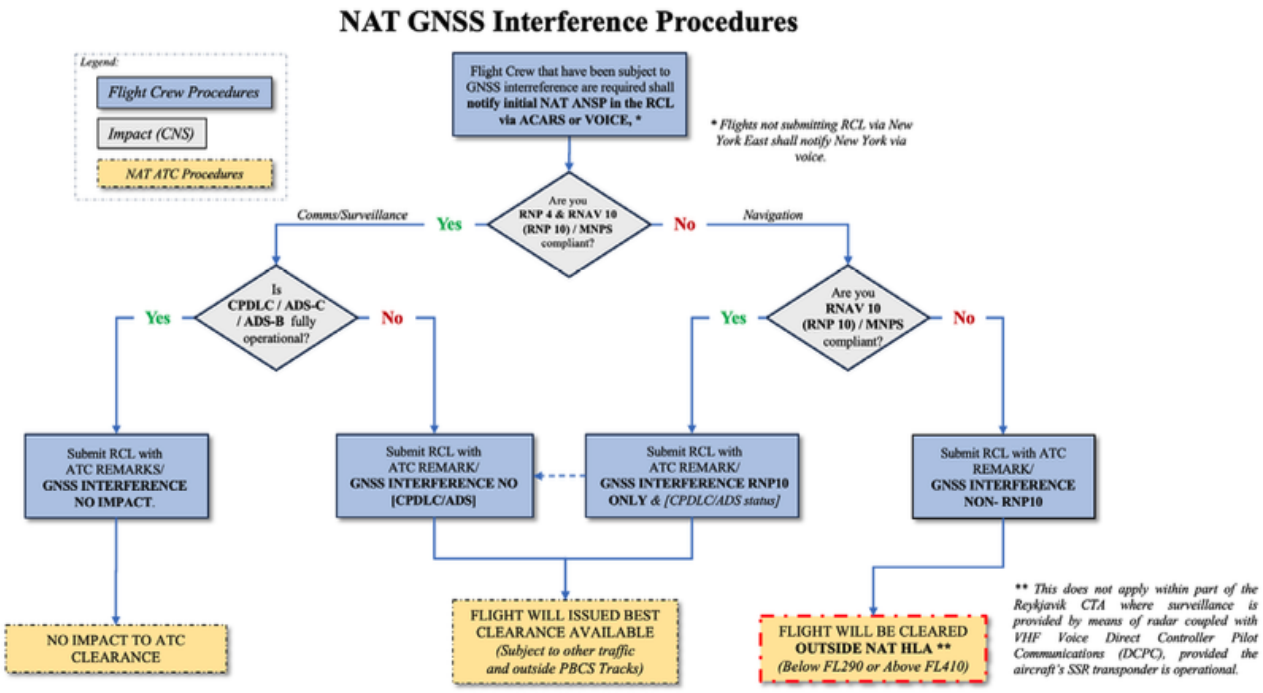
**‘ATC REMARKS/GNSS INTERFERENCE NON-RNP10**

By including your status in the RCL, you are **giving ATC a head’s up before you arrive.**

**In most cases, you will still be allowed in the NAT HLA.** A loss of RNP 4 isn’t a deal breaker, as you can still enter under RNP 10. But your clearance may be less optimal (likely level changes) due to the increased separation from other traffic.

**The big one to look for is a loss of RNP 10.** You will not be cleared into the NAT HLA, and instead will need to remain below FL290 or above FL410. With an obvious fuel impact, this may lead to an unplanned diversion.

The Bulletin includes a handy flow chart that’s worth printing and keeping in your flight bag.




Click for PDF.

### Latest ICAO Feedback

The latest three-yearly ICAO Assembly was held in Montreal from Sep 23 – Oct 3.

During the event, ICAO issued its strongest condemnation yet of both **Russia and North Korea**, directly blaming them for **deliberate GNSS interference** in violation of the Chicago Convention. Russia, in particular, has been blamed by ICAO for **destabilising navigation across European airspace.**

We continue to receive regular reports from OPSGROUP members of both jamming and spoofing. Interference is now a regular occurrence in the **Baltic region, particularly around Kaliningrad, Eastern Finland, the Baltic Sea, and nearby airspace.** Other reports have been received from **Germany, Poland and Norway.**

Recent airspace incursions, airstrikes and drone activity associated with the **ongoing conflict in Ukraine** have almost certainly escalated the use of GPS interference as a defensive measure. Civil aviation will continue to operationally grapple with this hazard. **With no obvious solution in site, our best defence remains procedures like the one detailed above.**

---

# Worldwide GPS Dual Failure mystery solved

OPSGROUP Team
21 October, 2025

The mystery of the dual GPS failures around the world has been solved.

Last week, a slew of Dual/Complete GPS Failures began to be reported by airlines and AOs around the world. A peak of failure reports were received around May 21. Typically, the fault was first annunciated as an “ADS-B RPTG” Fault, followed by GPS 1/2 failure. Aircraft affected were mostly B737 and A320 series, though some widebodies also caught the lurgy.

Initially, no clear cause could be established. There were theories about new spoofing and jamming areas, solar flares, sunspots, and troubling new hacker activity. But none of those lined up with the symptoms.

However, over the weekend, the culprit was traced to a single faulty satellite, GPS PRN 37. Data from the broadcast of this satellite led to the on-board failures that we saw.

Thanks to all OPSGROUP members that assisted with the “ALL CALL” that went out on Friday, there was a great response and we were able to collect a great deal of information. An Ops Alert was issued to members on Sunday, which reads:

**ZZZZ/Worldwide - Hazard** The mystery of worldwide dual GPS failures appears to have been solved. Over the weekend Boeing, Honeywell, and Collins collaborated to investigate the cause, and the outcome is that the faults were traced to one GPS satellite (PRN 37). A change in the data format being broadcast from it apparently led to the receiver failures. These were limited to Honeywell MMR's, predominantely on B737 and A320 series aircraft. This change has been corrected, and no further issues are expected. There was no connection to an increase in solar activity, or jamming/spoofing. The three OEM's involved consider the case closed. Thank you to all members who responded with reports and information.

A **special briefing** is in your member Dashboard, which includes crew reports of the issue.

### NANU NANU

There was a warning (published as a NANU message) to GPS users published earlier in the year, that warned of unhealthy navigation messages being broadcast on GPS satellites 35, 36 and 37 throughout 2025. Let’s hope that any rogue signals from PRN 35 or 36 don’t have the same effect down the track.

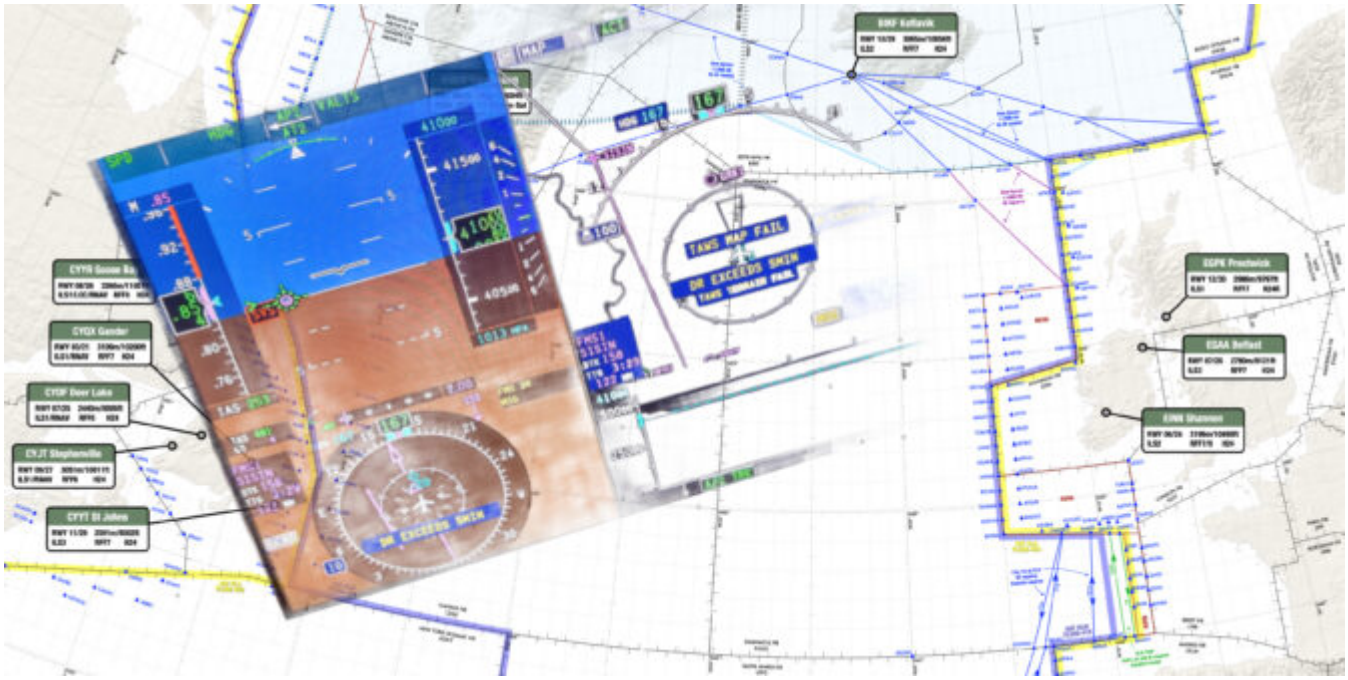
```
NOTICE ADVISORY TO NAVSTAR USERS (NANU) 2025017 NANU TYPE: GENERAL
*** GENERAL MESSAGE TO ALL GPS USERS ***
Testing will be occurring through CY 2025 using PRNs 35, 36, 37
on residual SVs broadcasting UNHEALTHY navigation messages.
*** GENERAL MESSAGE TO ALL GPS USERS ***

POC: CIVILIAN - NAVCEN AT 703-313-5900, HTTPS://WWW.NAVCEN.USCG.GOV
MILITARY - GPS WARFIGHTER COLLABORATION CELL at
HTTPS://GWCC-WS.CCE.AF.MIL/GPSOC, DSN 560-2541, COMM 719-567-2541,
gpsoperationscenter@us.af.mil, HTTPS://GWCC-WS.CCE.AF.MIL
MILITARY ALTERNATE - JOINT SPACE OPERATIONS CENTER, DSN 276-3526.
COMM 805-606-3526. JSPOCCOMBATOPS@US.AF.MIL
```

---

# NAT Crossing after GPS spoofing: a guide

Mark Zee
21 October, 2025




An increasing issue for the NAT Oceanic FIR's is how to handle aircraft with an in-flight degradation of GPS. This normally follows a **GPS Spoofing encounter** somewhere prior to Oceanic Entry, leading to a degraded RNP capability.

If you run into GPS issues before entering the Ocean, you will likely end up with RNP10 as the best you can manage for navigational accuracy. This presents some issues for the Oceanic controllers, as RNP4 is commonly used to ensure separation. We'll take a look at some scenarios and how to best handle these.

### Normal RNP requirements on the NAT

NAT Doc 007 specificies two RNP options for entry into the NAT HLA.

The first is **RNP10** (accuracy of 10 nm, 95% of the time). An important consideration here is that **RNP10 is really RNAV10**, but they call it RNP10 to keep things simple [See NAT Doc 007, 1.3.4]. The critical difference is that for RNAV10, on-board monitoring is not required. Since this can only be done by GPS, that's an important relief when it comes to spoofed flights.

The other is **RNP4** (accuracy of 4nm, 95% of the time). RNP4 is only an absolute requirement for PBCS Tracks ("Half-Tracks"). In practice, ATC commonly uses RNP4 for separation purposes on the NAT (Since the introduction of ASEPS). GPS is required for the monitoring part of RNP4; without GPS, RNP4 is not possible.

### Loss of GPS Prior to the NAT

Since GPS Spoofing became prevalent in September of 2023, increasing numbers of aircraft are arriving at the Oceanic Boundary with one or both GPS sensors inoperative. A textbook GPS Spoofing encounter will initially see the GPS sensors rapidly change from the real coordinates to fake coordinates. If all GPS sensors agree on the fake coordinates, the FMS becomes confused. IRU values will increase, and in some cases, the IRS may also become "infected".

The primary spoofing locations have not changed much since the onset of the issue: you will encounter spoofing at the Iraq/Iran border, the Sinai peninsula area (showing Tel Aviv as the spoofed location), Israel and Cyprus (showing Beirut as the spoofed location), and the Black Sea (showing Sevastopol as the spoofed location).

We have no reports in OPSGROUP that the other type of GPS interference – GPS Jamming – leads to lasting effects. Once the jamming has stopped, aircraft systems are normal.

However, we do have reports that if GPS inputs are turned off before departure, and later turned back on in flight, that issues may occur. This is mostly reported for departures from Tel Aviv (LLBG).

### GPS failure, Ocean approaching

Since RNP4 requires a functioning GPS, if you encounter spoofing and lose your GPS, you can't fly RNP4. Assuming that you have an RNP10 approval (one of the only two options for the NAT HLA), you will become **RNP10**.

The problem occurs when Shanwick, or the OACC at the entry point, get late notice of this fact, and you are close to other aircraft. That leaves the Planning Controller with little time to figure out how to separate you (an RNP10 aircraft) from the others (RNP4 aircraft).

In some cases, "spoofed" aircraft have had to descend  to FL280 to exit the NAT HLA, and this has caused diversions.

### How to best handle a NAT crossing with a failed GPS

The key is to advise Shanwick, or the first OACC, **early**. Shanwick's preference is that you use the RCL request to do this, and add a note to the end of the RCL along the lines of ATC REMARK/GPS DEGRADED RNP10 ONLY. If using voice to get your clearance, that's what to say as well. Shanwick NOTAM EGGX G0106/24, and a note on the OTS Track message, has this information.

The RCL for Shanwick should ideally be sent **90 minutes** before the Oceanic Entry in this case. Normal RCL timeframes are -30 to -90. An RCL sent any earlier will be rejected, but if you have something more unusual to discuss, you could use SATCOM to contact the supervisor and ensure a smooth crossing.

### RNP10 time limit

With the change to RNP10 for your crossing, double check the **time limit** for RNP10. ICAO Doc 9613 (Volume II, Part B, Chapter 1) specifies that RNP is limited to 6.2 hours of flying. The timing starts from when "the systems are placed in navigation mode" or at the last point at which the "systems are updated". The logic here is that the IRS will drift without updates enroute, and after 6.2 hours of flying, will no longer be capable of maintaining the RNP10 accuracy.

For an aircraft spoofed in the Mediterranean, or Black Sea area, it will take 4 hours before Oceanic entry, so this time limit becomes relevant. If the impact of the spoofing is severe enough, there is potential for inputs – including DME/DME or VOR/DME – to the IRS to stop working. This is one of the potential unknowns at present.

### Shanwick comments

Shanwick are encountering several GPS jammed aircraft per day, and it is sometimes difficult (or impossible) to find optimum profiles for aircraft without moving several other aircraft to accommodate. The only instance where they have to insist on FL280 and below, is when an aircraft does not meet the requirements for MNPS (such as single LRNS), and needs to be cleared outside HLA.

If a pilot advises that they have lost RNP4, but are still capable of RNP10, Shanwick controllers will look to find a solution where the aircraft can be cleared with at least 10 minutes longitudinal and 60nm lateral separation. These aircraft also need coordinating with the next Oceanic Center before clearance, and sometimes there are limited options available.

In general, the earlier they informed about the degradation, the easier it is for the Shanwick controllers to find satisfactory solutions.

### Member input

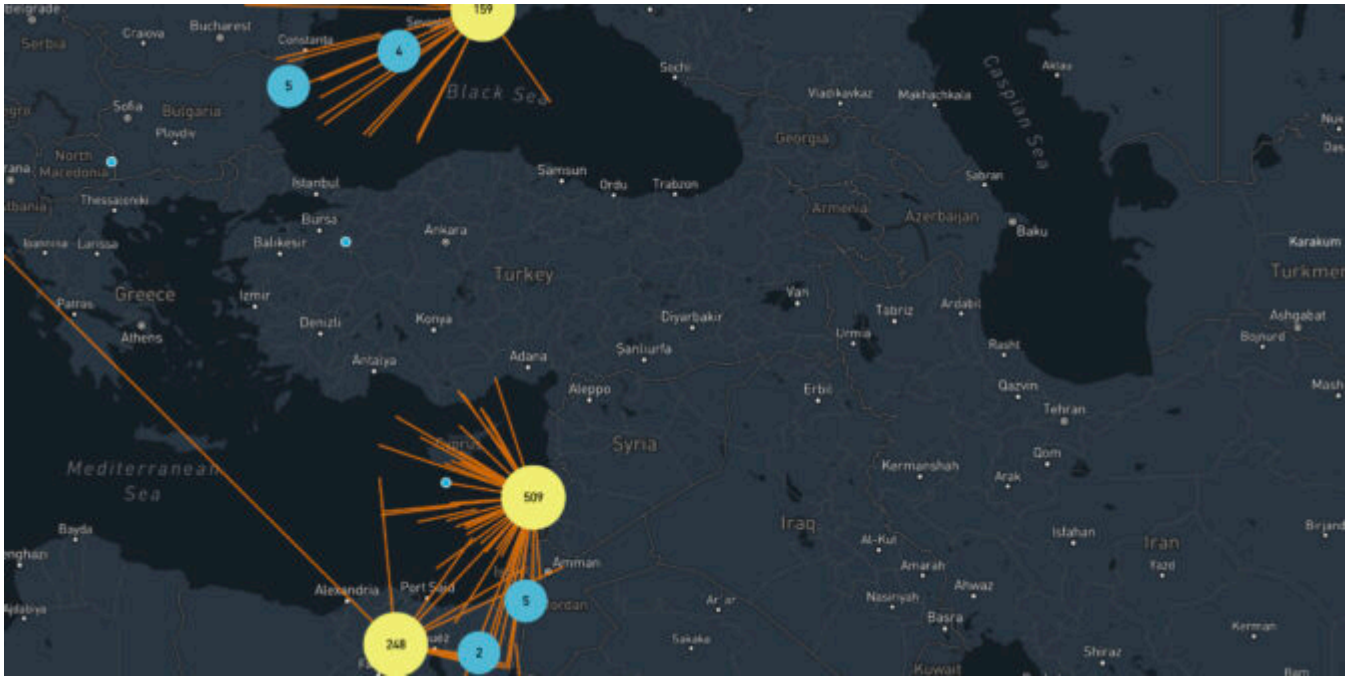
This is a developing issue and we gratefully welcome any input from members on this. Email us at **team@ops.group**.

---

# Where is the spoofing today? Two maps to

# help

Mark Zee
21 October, 2025

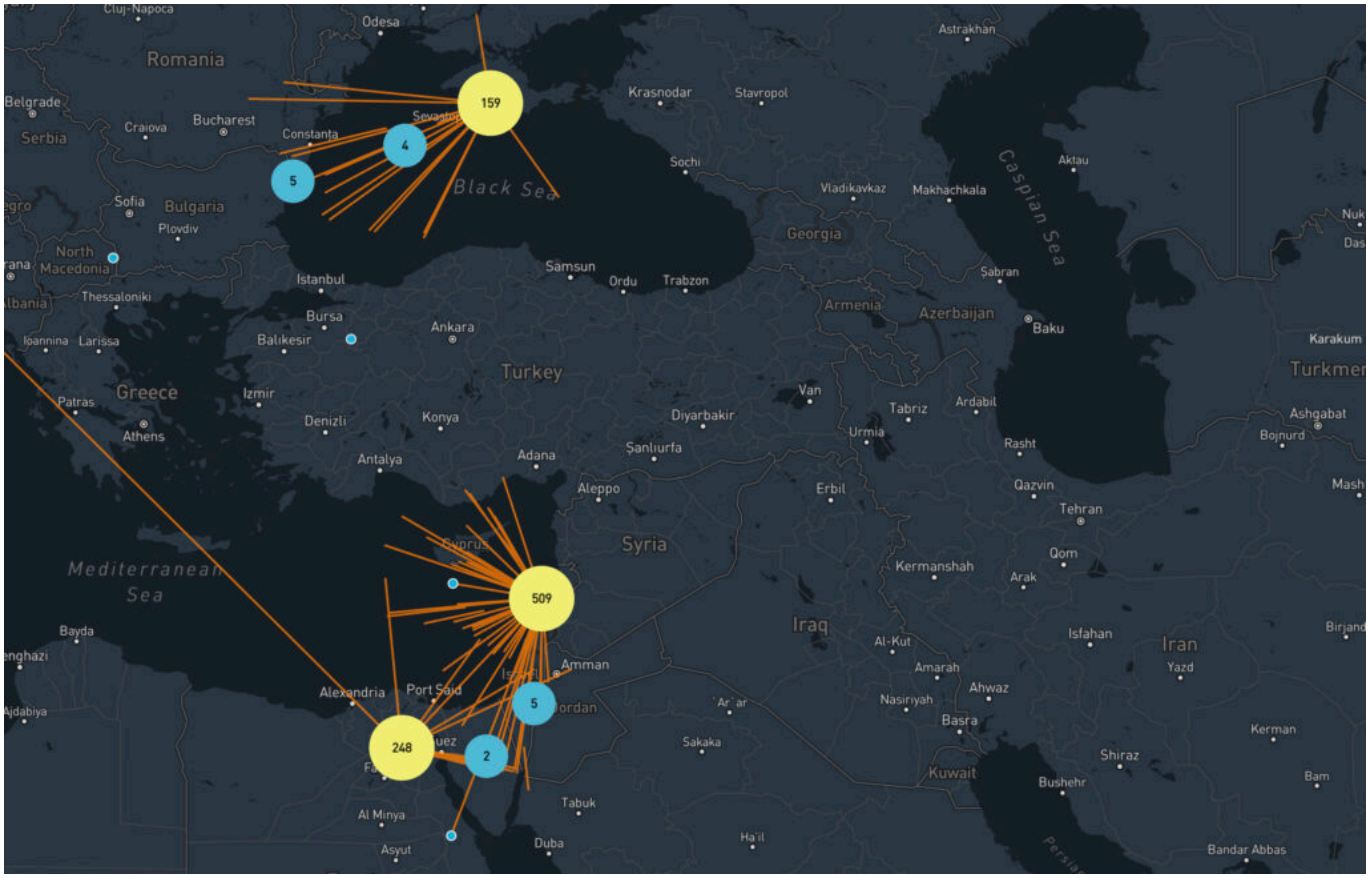



If you're keen to know exactly where GPS Spoofing – or GPS Jamming – might be happening today, there are two handy live maps to share with you.

Both of these use data from flight tracking websites to look for position anomalies, and convert those into hotspots that show where the activity is.

These are very useful in-flight to get a heads up on where you might encounter issues with GPS interference.

### Live GPS Spoofing tracker



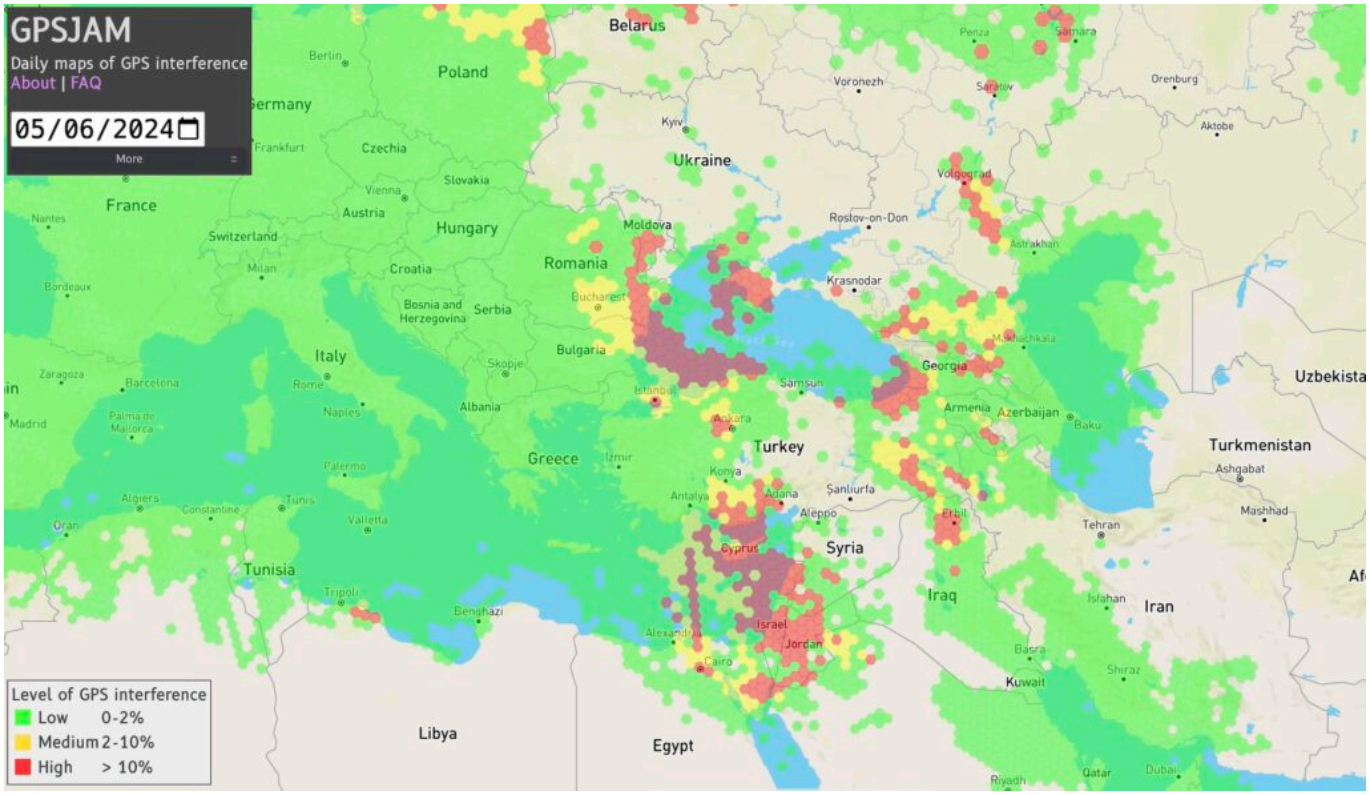

First up is this live **GPS spoofing tracker** from SkAI Data Services, in partnership with the Zurich University of Applied Sciences.

About a month ago, SkAI and Zurich University were following the discussions about GPS spoofing, and wondered if they could detect spoofing in real-time based on the ADS-B data from the OpenSky Network. As it turns out, they can. Having up-to-date information can help raise the situational awareness and prepare the flight crew for the possibility of spoofing.

Their algorithm can detect spoofing anywhere in the world where they have ADS-B coverage. The website is free to use. Unfortunately, the receiver network doesn't quite have the same coverage as other ADS-B websites, let alone space-based ADS-B. Regardless, it's a great tool for planning flights into areas of potential GPS issues.

The screenshot above is from this morning, May 7th. It matches exactly the three primary GPS spoofing hotspots this year: **Sevastopol**, **Beirut**, and **Cairo**. These are the three locations that you can expect your GPS to "think" it's at, when you are over the Black Sea, Eastern Med/Israel, and Egypt, respectively.

### GPS Jamming tracker




This map has been around a little longer, and will be familiar to some. GPS Jam uses data from ADS-B Exchange, and looks for aircraft indicating low navigation accuracy. More details are in their FAQ.

This was created when jamming was the only type of GPS interference we encountered, but now that spoofing is on the scene, it most likely shows both jamming and spoofing. That said, when being spoofed, the aircraft doesn't know it has an issue with navigation accuracy (and that's the very problem). Maybe someone knows more about this.

Either way, it's a great map to see potential GPS trouble spots.

### What's the latest on GPS Spoofing?

The spoofing tracker above is probably the best answer to that!

Since OPSGROUP first reported the new GPS Spoofing phenomenon in September last year, we continue to receive daily reports of spoofing. However, the areas affected remain largely the same. Our GPS Spoofing Pilot QRH from November last year still holds true, except that we've seen far fewer reports from the Iraq/Iran area, and a new area in Sevastopol affecting Black Sea transits.

We continue to ask members to report GPS spoofing events (pictures are very useful too) to us at team@ops.group, or via WhatsApp to +1 747 200 1993. Thank you!

---

# FAA warning issued, further serious

# navigation failures reported

OPSGROUP Team
21 October, 2025

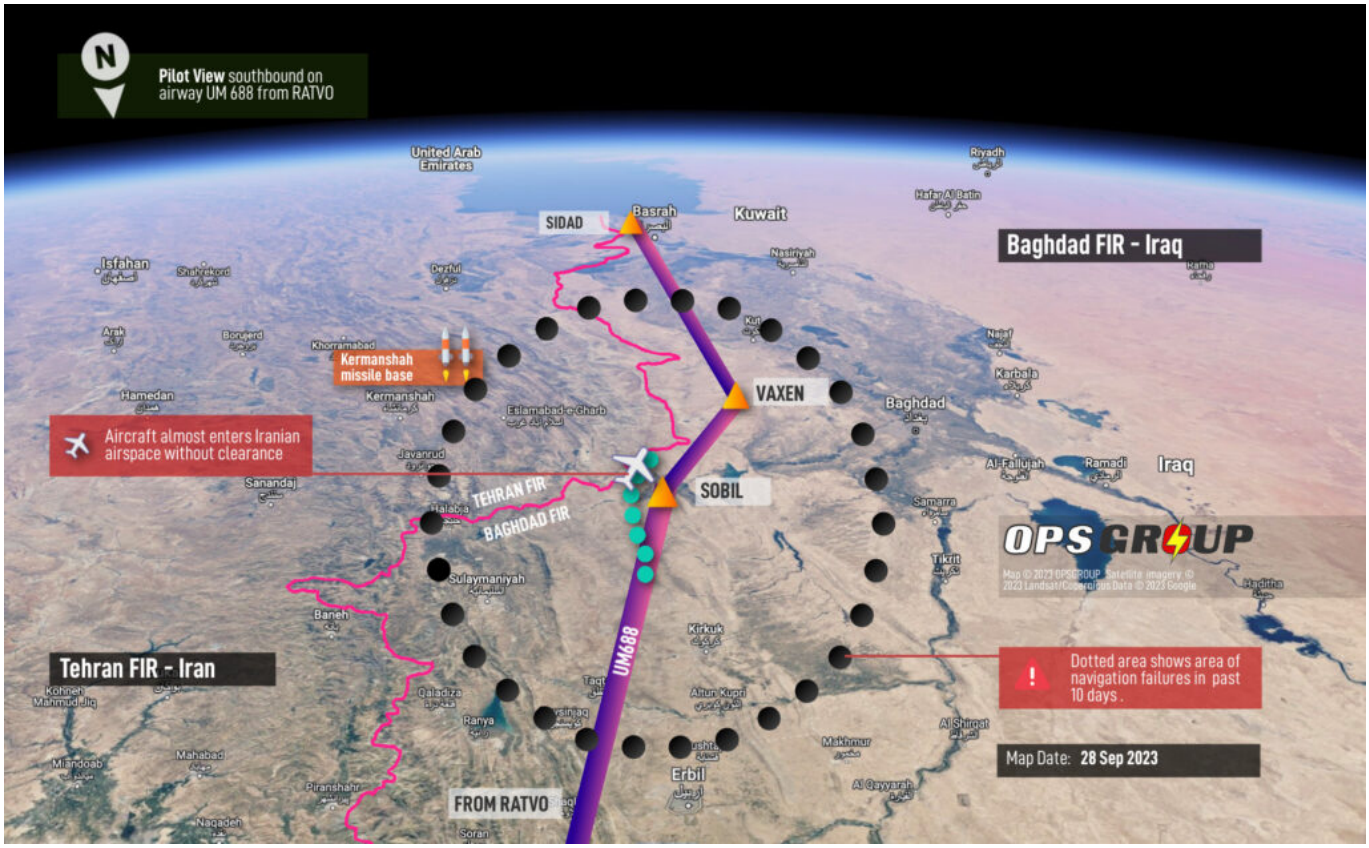

Since publishing Monday's **risk warning** on complex navigation failures following fake GPS signals, we have received further concerning reports from operators, mirroring the same events. The impact of the nav failures is becoming clearer, with one operator **almost entering Iranian airspace without clearance**, and another left **requiring ATC vectors all the way to their destination in Doha**.

In total we now have **20 reports** of almost identical situations. Full reports are in **Version 2** of our **Risk Warning** (PDF), see further down.

On Wednesday evening, the **FAA issued a warning memo** to aircraft operators as a result of the situation, warning of increased "safety of flight risk to civil aviation operations".

### Embraer Legacy 650: We nearly entered Iran airspace with no clearance

One of the new reports received since Monday was from an Embraer 650 crew enroute from Europe to Dubai. They tell us, "In Baghdad airspace, we lost both GPS in the aircraft and on both iPads. Further, **the IRS didn't work anymore**. We only realized there was an issue because **the autopilot started turning to the left and right**, so it it was obvious that something was wrong. After couple of minutes we got error messages on our FMS regarding GPS, etc. So we had to request radar vectors. We were showing about 80 nm off track. **During the event, we nearly entered Iran airspace (OIIX/Tehran FIR) with no clearance.**




### Challenger 604: Required vectors all the way to Doha

Another new crew report received since our first warning informs us: “Nearing north of Baghdad something happened where we must have been spoofed. We lost anything related to Nav and the IRS suggested we had drifted by 70-90 miles. We had a ground speed of zero and the aircraft calculated 250kts of wind. The FMS’s reverted to DR (Dead Reckoning) and had no idea where they were.

We initially took vectors to get around the corner at SISIN. Nav capability was never restored, so **we required vectors all the way from Iraq to Doha for an ILS**. We never got our GPS sensors back until we fired up the plane and went back to home base two days later.

### Concern grows over flight risk

With these additional reports, OPSGROUP has increased concerns over the situation:

- **Security risk**: Navigation failures are occuring in close proximity to the Iranian border. One aircraft reported almost straying into Iranian airspace (Tehran FIR, OIIX) without a clearance. This area of the border is considered sensitive by Iran: there are two large missile bases just across the boundary: one at **Kermansah** (a huge facility with dedicated anti-aircraft weapons), and another at **Khorramabad**. For context, Iran shot down a passenger aircraft in 2020 in Tehran (accidentally), and has been heard in September 2023 **issuing warnings on 121.5** with threats to shoot down aircraft entering the FIR without a clearance.
- The **Navigation failures are severe**. The second report above highlights how the crew had no option but to request radar vectors – all the way to their final destination. In many other reports, most aircraft have no reliable on board navigation, for periods of 20-30 minutes and in some cases an hour or more.

- **Compounding failures**. Individually these incidents can mostly be resolved with the help of ATC. Consider however, an ATC comms failure, ATC radar failure, or an emergency situation: engine failure, decompression, or even a medical divert. The workload would quickly become extreme, and diverting at night (when most flights are transiting the area) without basic navigation capability is not a scenario we want to deal with.
- **Inadequate guidance for crews**: Current FCOM/AOM procedures available to aircrew are insufficient to capably deal with this new GPS spoofing issue. Having been shown to be possible, there is potential for it to occur elsewhere in the world.

#### FAA warning issued

On Wednesday evening, the FAA released a memo for aircraft operators titled "**Iraq/Azerbaijan – GPS Jamming and Spoofing Poses Safety Risk**"."

The memo advised that "**Potential spoofing activities reported by various civil air operators in Iraq and Azerbaijan pose a safety of flight risk to civil aviation operations** in the Baghdad (ORBB) and Baku (UBBA) Flight Information Regions (FIR)."

"The recent opensource reporting regarding spoofing incidents, if confirmed, would pose increased safety of flight risks, due to potential loss of aircraft situational awareness and increased pilot and regional air traffic control (ATC) workload issues, which can lead to potential accidents and/or loss of life."

**"FAA recommends that U.S. civil air operators transiting ORBB and UBBA** monitor regional NOTAMs, put additional emphasis on maintaining continuous communications with appropriate air traffic control authorities while **monitoring aircraft equipment performance closely for any discrepancies or anomalies**, and to be prepared to operate without GPS navigational systems."

## Geopolitical background, analysis from experts

Earlier, Matthew Borie of **Osprey Flight Solutions** provided background context for our members: "Iran has recently deployed additional military forces to its northwest border with the Iraqi Kurdistan Region and Iraq has deployed security forces to this area as well as part of a border security pact reached between the two countries in March. Both the Iran and Iraq have Electronic Warfare equipment capable of GPS jamming and spoofing and may have these deployed to the northern border area.

The US military is present at several bases in northern Iraq (Erbil, Harir & Sulaymaniyah). Turkey has military bases on its side of the Iraq border as well as inside Iraqi territory in several areas (Amadiya, Harkuk & Bashiqa). These deployments are enduring and not new – both the US and Turkey have electronic warfare (EW) equipment capable of GPS jamming and spoofing and they may have these deployed to Iraq.

Iran has also recently deployed additional military forces to its northwest borders with Armenia and Azerbaijan in wake of the Azerbaijani military operation in Nagorno-Karabakh. In addition, tensions between the Armenian military and Azerbaijani armed forces remain high on the border between the two countries at present in wake of the Azerbaijani military operation in Nagorno-Karabakh. Iran, Armenia and Azerbaijan all have EW equipment capable of GPS jamming and spoofing and may have these deployed to border areas"

An intelligence brief from **Dyami Intelligence Services** issued in repsonse to Monday's reports, adds information about this new form of GPS spoofing affecting aircraft: "The surge in GPS jamming and spoofing incidents within the Iraqi FIR, along with their widespread occurrences, strongly indicates the involvement of an airborne platform (UAV). In the past, Iran has successfully intercepted a drone by GPS spoofing. Spoofing provides an attack vector that enables control over the target UAV (aircraft) without compromising the flight control software or the command-and-control radio link. Furthermore, a GPS spoofing attack can be carried out by an attacker who is equipped with an RF transmitter that can be ground or airborne-based."

## This is not jamming: Inadequate NOTAMs

It's clear in the initial discussions of these events that because we are used to GPS jamming, crews may make make the initial assessment that these are the same routine GPS jamming events. While there are NOTAMs issued for many FIR's in the region, they only warn of the routine GPS jamming that crews have experienced since 2018 in the Middle East and Mediteranean areas.

The **key difference** between the jamming events we are used to, and these **new GPS spoofing attacks** is the rapid impact on our on-board navigation. Some very alert crews have been able to quickly de-select GPS and isolate the input, but for most – and depending on aircraft and avionics types – this has not been possible. In the vast majority of the pilot reports received, crews have had to resort to radar vectoring from ATC.

**OPSGROUP calls on the Iraqi CAA** to issue a **new NOTAM warning crews of the specific risk of complete navigation failure**, due to spoofed GPS signals that many aircraft systems interpret as valid information.

## Aircraft manufacturer and avionics responses

OPSGROUP has received confirmation from several aircraft manufacturers involved that they are taking the issue very seriously, and are working on a solution. We will keep members updated on this.

**Bombardier** is actively working on a new FON (Flight Operations Notification ) concerning GNSS Spoofing; we will keep members updated on this once we hear more from them.

## "The IRS can't be spoofed" – until it can

Quite astonishing for many of us as flight crew is the idea the IRS (Inertial Reference System) can be subject to outside interference.

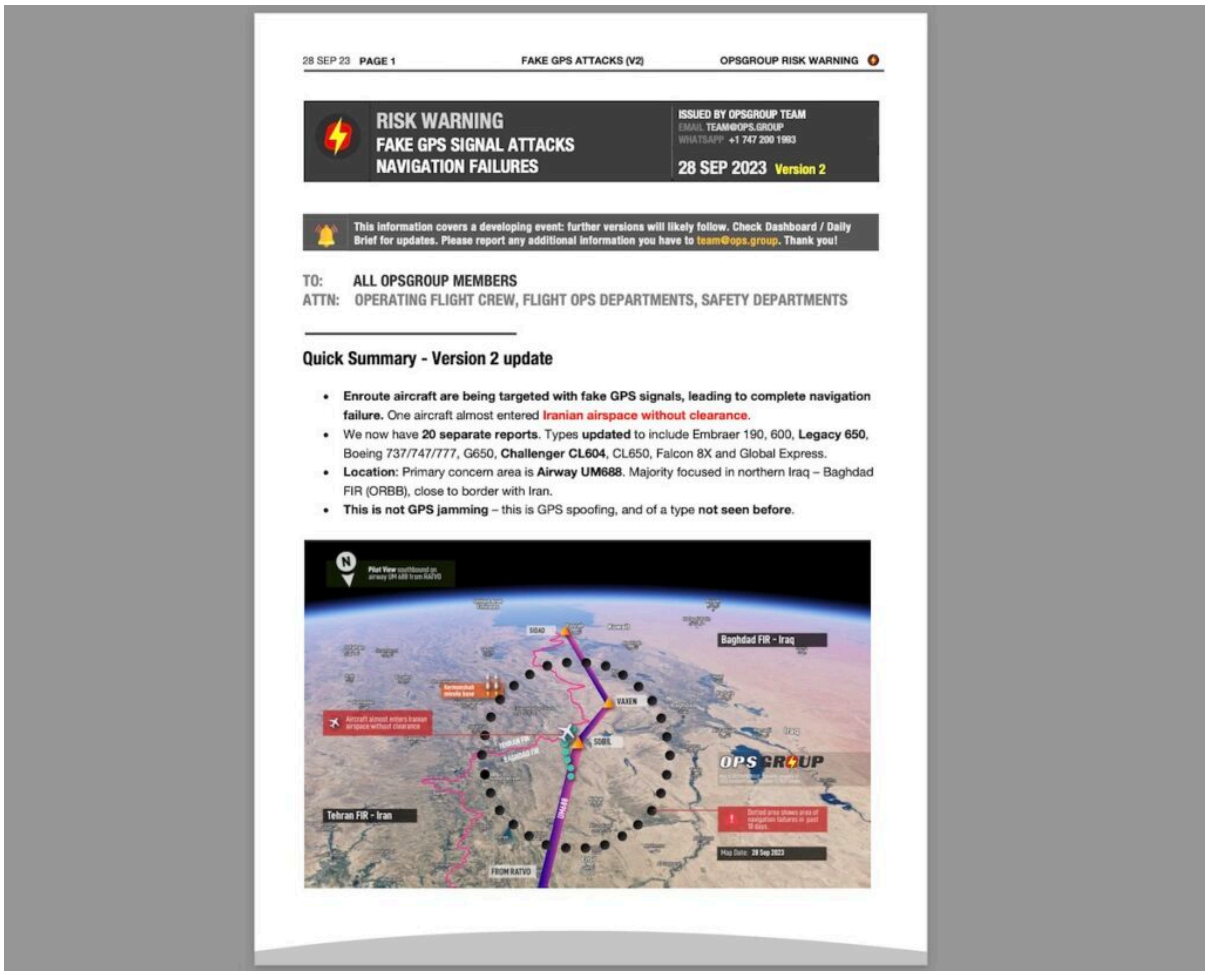
Exactly where the avionics problem arises as a result of these GPS spoofing signals is something that OEM's and Avionics providers are working on. However, **many modern IRS platforms include GPS updating while enroute, to correct drift**.

Previously, jammed or degraded GPS signals were neatly ignored with no impact on the IRS. What seems to be happening in these cases, is that the spoofed GPS position is a strong signal, and the IRS doesn't know that it's incorrect. The technical details are unclear, and we await clarification from subject experts on this.

Regardless of exactly what is happening internally, the impact on navigation systems is clear.

**OPSGROUP Member resources – update**

**Updated version** of **Risk Warning: Fake GPS Signal attacks (28SEP/V2)** is now available in your Dashboard.



28 SEP 23 PAGE 1 FAKE GPS ATTACKS (V2) OPSGROUP RISK WARNING

**RISK WARNING**
**FAKE GPS SIGNAL ATTACKS**
**NAVIGATION FAILURES**

ISSUED BY OPSGROUP TEAM
EMAIL TEAM@OPS.GROUP
WHATSAPP +1 747 200 1983
28 SEP 2023 Version 2

This information covers a developing event: further versions will likely follow. Check Dashboard / Daily Brief for updates. Please report any additional information you have to team@ops.group. Thank you!

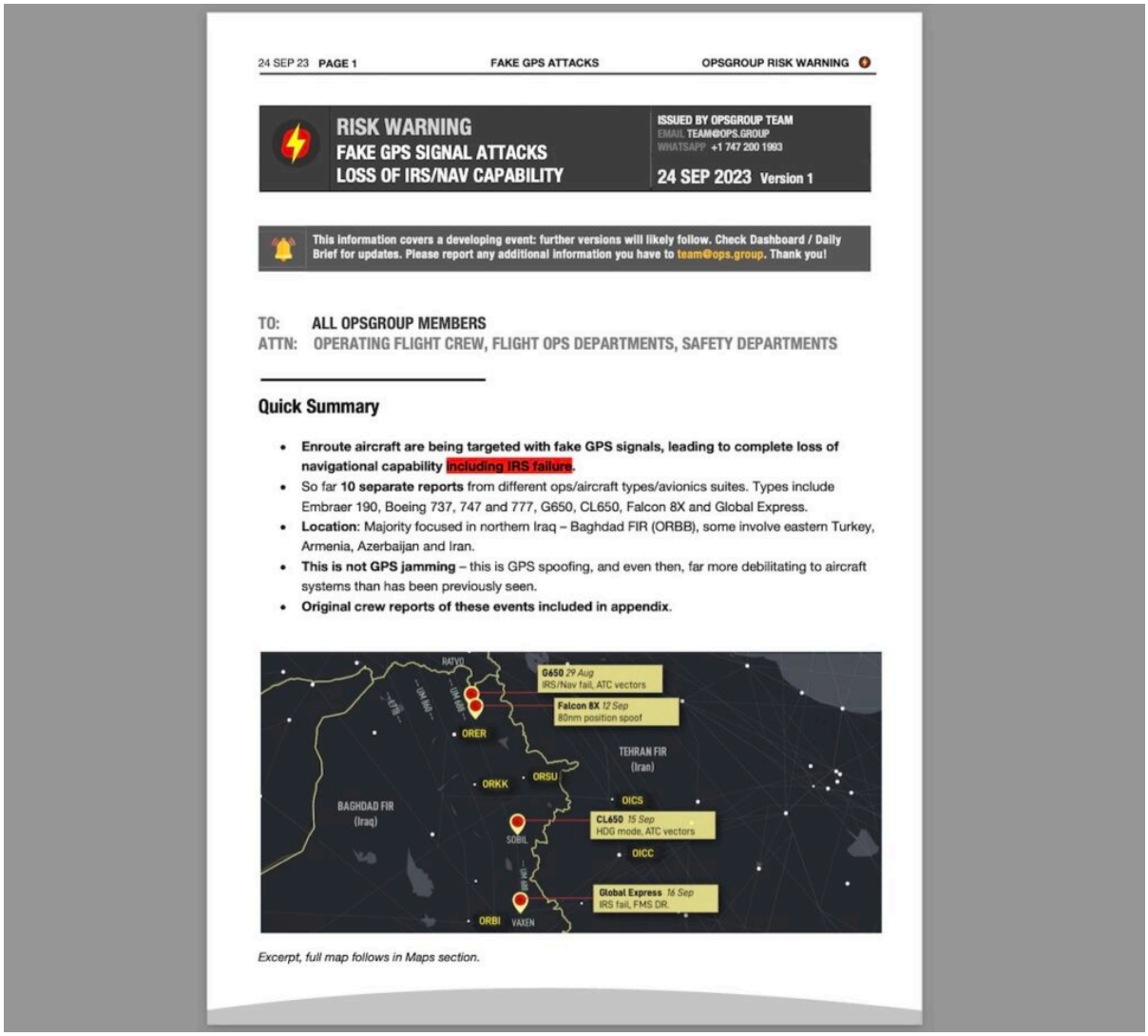
TO: ALL OPSGROUP MEMBERS
ATTN: OPERATING FLIGHT CREW, FLIGHT OPS DEPARTMENTS, SAFETY DEPARTMENTS

**Quick Summary - Version 2 update**

- **Enroute aircraft are being targeted with fake GPS signals, leading to complete navigation failure.** One aircraft almost entered **Iranian airspace without clearance**.
- We now have **20 separate reports**. Types **updated** to include Embraer 190, 600, **Legacy 650**, Boeing 737/747/777, G650, **Challenger CL604**, CL650, Falcon 8X and Global Express.
- **Location:** Primary concern area is **Airway UM688**. Majority focused in northern Iraq – Baghdad FIR (ORBB), close to border with Iran.
- **This is not GPS jamming** – this is GPS spoofing, and of a type **not seen before**.



Earlier version: OPSGROUP members provided analysis of the events, and recommended guidance. This work has been collated into **Briefing: RISK WARNING 24SEP/V1**, available to all members in your Dashboard. Direct links are below.



24 SEP 23 **PAGE 1** FAKE GPS ATTACKS OPSGROUP RISK WARNING

**RISK WARNING**
**FAKE GPS SIGNAL ATTACKS**
**LOSS OF IRS/NAV CAPABILITY**

ISSUED BY OPSGROUP TEAM
EMAIL TEAM@OPS.GROUP
WHATSAPP +1 747 200 1993
**24 SEP 2023** Version 1

This information covers a developing event: further versions will likely follow. Check Dashboard / Daily Brief for updates. Please report any additional information you have to team@ops.group. Thank you!

TO: ALL OPSGROUP MEMBERS
ATTN: OPERATING FLIGHT CREW, FLIGHT OPS DEPARTMENTS, SAFETY DEPARTMENTS

**Quick Summary**

- **Enroute aircraft are being targeted with fake GPS signals, leading to complete loss of navigational capability including IRS failure.**
- So far **10 separate reports** from different ops/aircraft types/avionics suites. Types include Embraer 190, Boeing 737, 747 and 777, G650, CL650, Falcon 8X and Global Express.
- **Location:** Majority focused in northern Iraq – Baghdad FIR (ORBB), some involve eastern Turkey, Armenia, Azerbaijan and Iran.
- **This is not GPS jamming** – this is GPS spoofing, and even then, far more debilitating to aircraft systems than has been previously seen.
- **Original crew reports of these events included in appendix.**



*Excerpt, full map follows in Maps section.*

- **Download** Briefing: RISK WARNING – **Fake GPS signal attacks** (PDF, 0.7 Mb)
  - Situation report
  - **Key information for Flight Crew**
  - Analysis from OPSGROUP members
  - **Original Crew reports** of GPS spoofing/Nav & IRS failures (First 10 reports listed)
  - **Guidance and Procedures**
    - Awareness of risk locations
    - Recommended Procedure – entering risk area
    - Recommended Procedure – active GPS spoofing

- **Download** : LOCATION MAP showing **report locations of Fake GPS signal attacks**

**Further information**

- Initial report: **Flights Misled Over Position, Navigation Failure Follows** (26 SEP)
- Contact **team@ops.group** or WhatsApp **+1 747 200 1993**

---

# Flights misled over position, navigation failure follows

Mark Zee
21 October, 2025



**Update – Thursday Sep 28**

Since publishing Monday's **risk warning** on complex navigation failures following fake GPS signals, we have received further concerning reports from operators, mirroring the same events. The impact of the nav failures is becoming clearer, with one operator **almost entering Iranian airspace without clearance**, and another left **requiring ATC vectors all the way to their destination in Doha**.


In total we now have **20 reports** of almost identical situations. Full reports are in **Version 2** of our **Risk Warning** (PDF).

On Wednesday evening, the **FAA issued a warning memo** to aircraft operators as a result of the situation, warning of increased “safety of flight risk to civil aviation operations”.

**See new Briefing (28SEP) – “FAA Warning Issued, Further Serious Navigation Failures Reported”**

*Original article follows:*

**Key points**

- **New RISK WARNING: Enroute aircraft are being targeted with fake GPS signals, leading to complete nav failures**
- **~~12~~ 16 separate reports – types include Embraer 190, 600, Boeing 737, 747 and 777, G650, CL605, CL650, Lear 45, Falcon 8X and Global Express.**
- **This type of GPS spoofing has not been seen before – IRS is quickly “infected” by false position**
- **OPSGROUP Members: Suggested Guidance and Procedures, and original crew reports, in Briefing PDF below**

## Situation

A troubling new development in enroute airspace is emerging: **aircraft are being targeted with fake GPS signals**, quickly leading to complete loss of navigational capability. **12 separate reports** have been now received by OPSGROUP, and **in most cases the IRS becomes unusable**, VOR/DME sensor inputs fail, the aircraft UTC clock fails, and the crew have been **forced to request vectors from ATC to navigate**.

Most reports have been in the last 7 days. Aircraft involved include various Boeing types (B777, B747, B737), Embraer (190, 600), Gulfstream 650, Challenger 650, Global Express, and a Falcon 8X. The location for the majority is also quite specific: Airway **UM688** in Iraq, close to the Iranian border.

This immediately sounds unthinkable. The IRS (Inertial Reference System) should be a standalone system, unable to be spoofed. The idea that we could loose all onboard nav capablity, and have to ask ATC for our position and request a heading, makes little sense at first glance – especially for state of the art aircraft with the latest avionics. **However, multiple reports confirm that this has happened**. The key issue appears to be the way the IRS uses GPS updates to update its position during flight. Analysis from other OPSGROUP members is contained in the Briefing (Risk Warning) below.

In the Baghdad FIR, the crew of a 777 enroute were essentially forced to ask "***What time is it, and where are we?*** ". Almost all incidents we've seen result in requiring ATC vectors to navigate. Clearly, in the areas that these events are occuring, this is disconcerting.

The location of reports received is mapped out below. The primary area of concern at the moment is **Airway UM688** in northern Iraq. Most crews have reported the nav failures in the vicinity of ORER/Erbil, ORSU/Sulaimaniyah, and ORBI/Baghdad.

It's important to highlight is that this **not traditional GPS jamming** – which we all experience almost as routine in these areas. We have become very used to GPS dropping out in Turkish and Iraqi airspace. These recent reports are GPS spoofing – and even then, **not like anything we've seen before**.

In most reports received, the situation plays out the same. **A spoofed GPS signal is directed at the aircraft**, or at least, received by the aircraft. The GPS position shifts by 60nm. The onboard systems start to react. Some crews have been able to quickly disable GPS inputs, but for the majority, the spoofed signal quickly leads to a nav failure.

One of the crew reports for an **Embraer 190** (see below), tells us, "*I have been on the aircraft for 13 years. I tried everything I know, but nothing helped. Two IRS's, which are updated from GPS, lost position. FMS disagree messages appeared. The main point is to disable GPS inputs at the very beginning of spoofing. If you miss a moment, you will lose navigation capability!*" This crew member is also Technical Pilot for the E190 type.

## Worrying scenario

Of all locations that we fly through, the one place we don't want to have any navigation issues would be

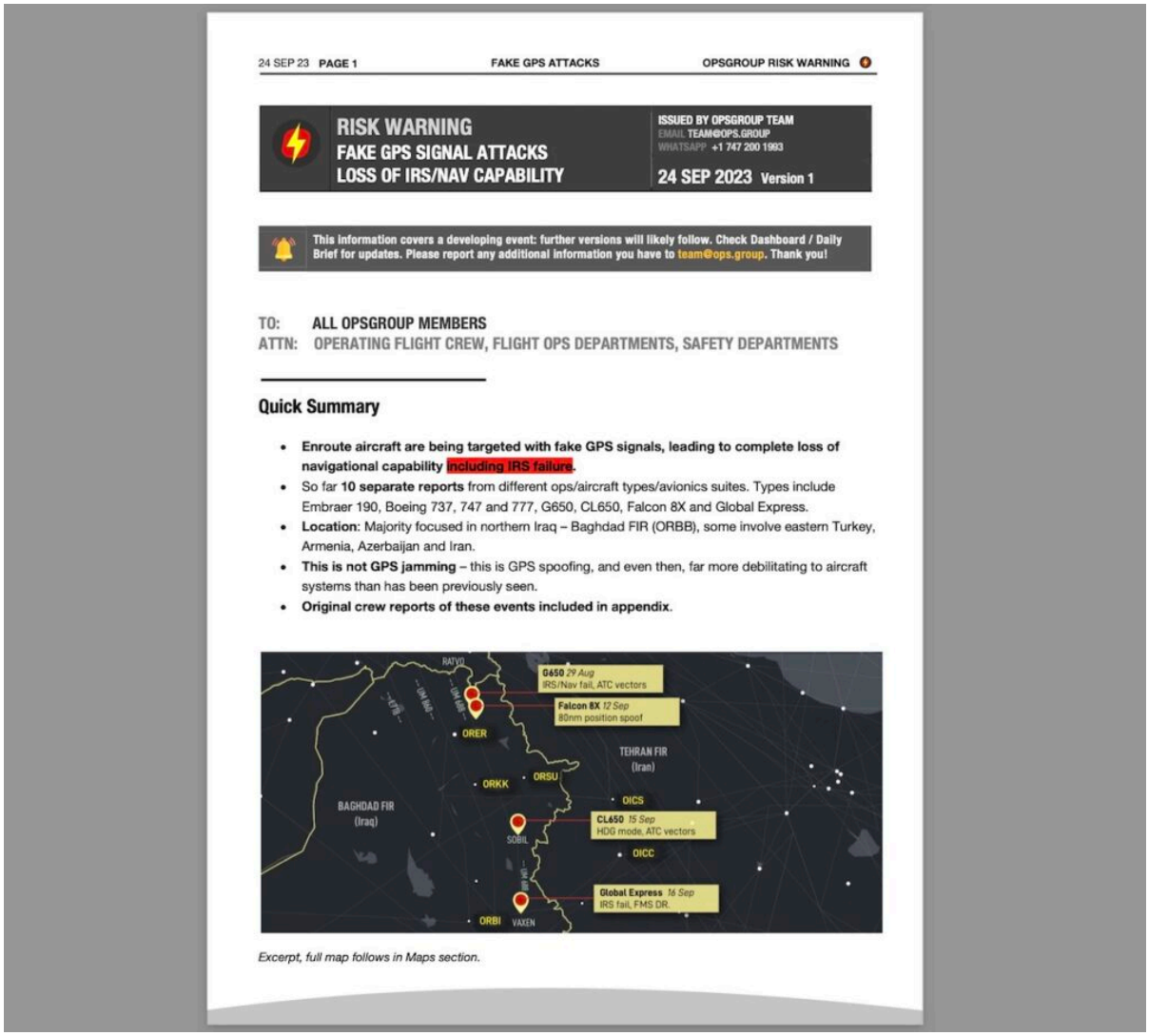
**along UM688**. This airway runs southbound through Iraq, **above an active conflict zone**, and extremely close to the border with Iran. Any indavertent straying into Iranian airspace without a flight plan risks action by the Iranian military.

And yet it is precisely here that most of these events in the last week have been happening. As such, **the risk to routine flight operations is extremely elevated**.

OPSGROUP recommends that all operators using airway **UM688**, or entering the Iraq/Iran/Turkey region, **review this new risk as soon as possible**. Flight Crew should be made aware of the potential for fake GPS signals, the likely impact on aircraft systems, and a plan of action should this occur.

#### OPSGROUP Member resources

Over this past weekend (23-24 September), OPSGROUP members provided analysis of the events, and recommended guidance. This work has been collated into **Briefing: RISK WARNING 24SEP/V1**, available to all members in your Dashboard. Direct links are below.



24 SEP 23 PAGE 1 FAKE GPS ATTACKS OPSGROUP RISK WARNING

**RISK WARNING**
**FAKE GPS SIGNAL ATTACKS**
**LOSS OF IRS/NAV CAPABILITY**

ISSUED BY OPSGROUP TEAM
EMAIL TEAM@OPS.GROUP
WHATSAPP +1 747 200 1993
24 SEP 2023 Version 1

This information covers a developing event: further versions will likely follow. Check Dashboard / Daily Brief for updates. Please report any additional information you have to team@ops.group. Thank you!

TO: ALL OPSGROUP MEMBERS
ATTN: OPERATING FLIGHT CREW, FLIGHT OPS DEPARTMENTS, SAFETY DEPARTMENTS

**Quick Summary**

- **Enroute aircraft are being targeted with fake GPS signals, leading to complete loss of navigational capability including IRS failure.**
- So far **10 separate reports** from different ops/aircraft types/avionics suites. Types include Embraer 190, Boeing 737, 747 and 777, G650, CL650, Falcon 8X and Global Express.
- **Location**: Majority focused in northern Iraq – Baghdad FIR (ORBB), some involve eastern Turkey, Armenia, Azerbaijan and Iran.
- **This is not GPS jamming** – this is GPS spoofing, and even then, far more debilitating to aircraft systems than has been previously seen.
- **Original crew reports of these events included in appendix.**



*Excerpt, full map follows in Maps section.*

- **Download** Briefing: RISK WARNING – **Fake GPS signal attacks** (PDF, 0.7 Mb)
    - Situation report

    - **Key information for Flight Crew**
    - Analysis from OPSGROUP members
    - **Original Crew reports** of GPS spoofing/Nav & IRS failures (First 10 reports listed)
    - **Guidance and Procedures**
        - Awareness of risk locations
        - Recommended Procedure – entering risk area
        - Recommended Procedure – active GPS spoofing

- **Download** : LOCATION MAP showing **report locations of Fake GPS signal attacks**

### IRS failures

An excerpt of analysis from the **Briefing Document** above helps us understand the issue better:

"Most avionics suites are now engineered such that the **IRS position is regularly GPS updated** to ensure the highest accuracy, if the GPS fails!

Therefore if the GPS is *jammed*, then the IRS works from its last known position. However if it receives a ***spoof position***, the system still believes the GPS input received to be accurate as all sources "say" the same thing, and this spoof position is then updated to the IRS(s) to match. Most avionics system know that a shift/gross-error has happened as ground based updates do not compute the correct position, and will flag a navigation/map/position warning.

However, all primary navigation systems end up being corrupted as a result. **It has the potential to be very dangerous**, and is part of the reason why pilots should back up navigation still, with "green needles" / ground based aids wherever possible. Our dependance on GPS is not always good!

I would recommend using conventional ground based navaids (DME/VOR/NDB) as far as practical, otherwise request assistance from ATC. Some platforms may allow IRS systems to be disconnected from GPS auto-updating, but most now do it in the background with no optional pilot interaction.

Unless the IRS systems are completely independent (the old fashioned ones that have to be initialised at startup location), GPS integration for frequent position updates, is sadly the issue due to its vulnerability to spoofing. For those that can disable the updating, they may wish to consider turning this function off, however it may impact on navigation capability, AFM requirements and operational approvals.

**I would recommend that pilots and operators reach out to their OEMs for their recommendations on dealing with spoofing on their platform."**

Another member (767 operator) spoke to an IRS expert for perspective – also arguing that "**the IRS system is "stand alone" and the only mixing between GPS and Inertial is inside the FMS and thus, the IRS couldn't be spoofed**. He assured me it could. Not enough to lose the alignment platform, but enough to confuse the present position and thus, none of the radio navaids are where they're supposed to be."

### Updates

This information covers a developing event: further versions will likely follow. Check your members Dashboard / Daily Brief for updates.

Much of the information is compiled from member feedback. If you have any expertise to share, or information to add – please email **team@ops.group**, or send a *WhatsApp* message to **+1 747 200 1993**.

Thank you!

---

# Signal Jam: US GPS Interference Testing This Month

Chris Shieff
21 October, 2025

For the remainder of March, the US military are carrying out GPS interference testing in three locations around the US for extended periods of time. During these periods, aircraft within 350nm of the tests may lose GPS signal completely – including **WAAS** and **ADS-B.**

Here's a quick summary of what's happening, and when.

### Wait. It ain't broken – why do they have to interfere with it in the first place?

Simply put, because the military need to be prepared if GPS signals are lost due to enemy jamming. That way it allows service personnel to train in an environment where it is not available.

In the event of a large-scale conflict, it is likely that the constellation of GPS satellites may be targeted or interfered with to erode the other's side's ability to navigate, deploy weapons accurately or even operate surveillance drones or other unmanned vehicles.

We've written about GPS jamming before – take a look at our article if you'd like to know a little more.

Unfortunately, aviation is forced to make way for these exercises. Despite being heavily dependent on GPS, the exercises simply have to happen. And in fact, they are happening more often than ever before. They are four times as frequent as they were just ten years ago.

### Back to what's happening this month.

There are **three tests** to be aware of (the range of outages increases with flight level).

*Southeastern US*

A Carrier Strike Group will be carrying out tests off the coast of South Carolina. Three days are affected:

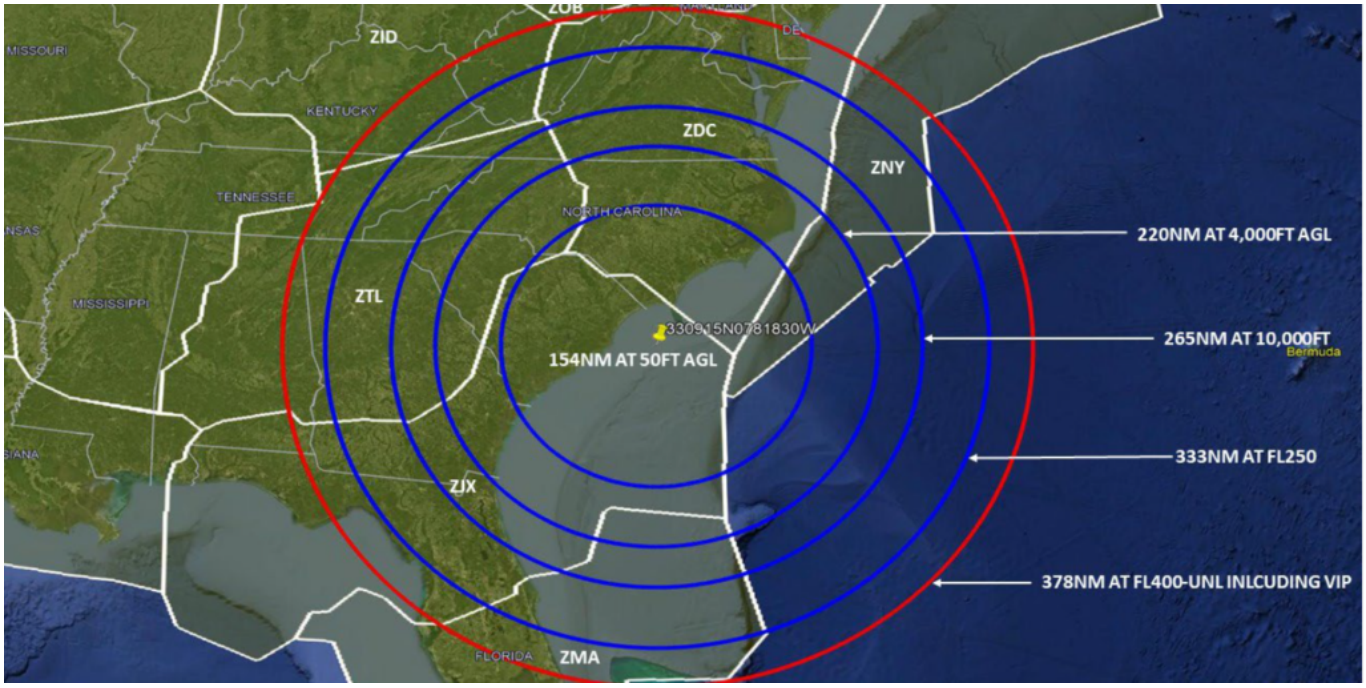
**15 March** 1900z – 2130z

**17 March** 1200z – 1630z

**28 March** 1200z – 1630z

……..*(Local time GMT-4)*

Here is a map of the affected area:



*South Carolina Courtesy: FAA*

More testing is happening over at Fort Irwin, California. The test days are much more frequent than the other side of the country:

**16 March** 0700z – 1259z

**18 March** 0700z – 1259z

**19 March** 0700z – 1259z  1830z – 2200z

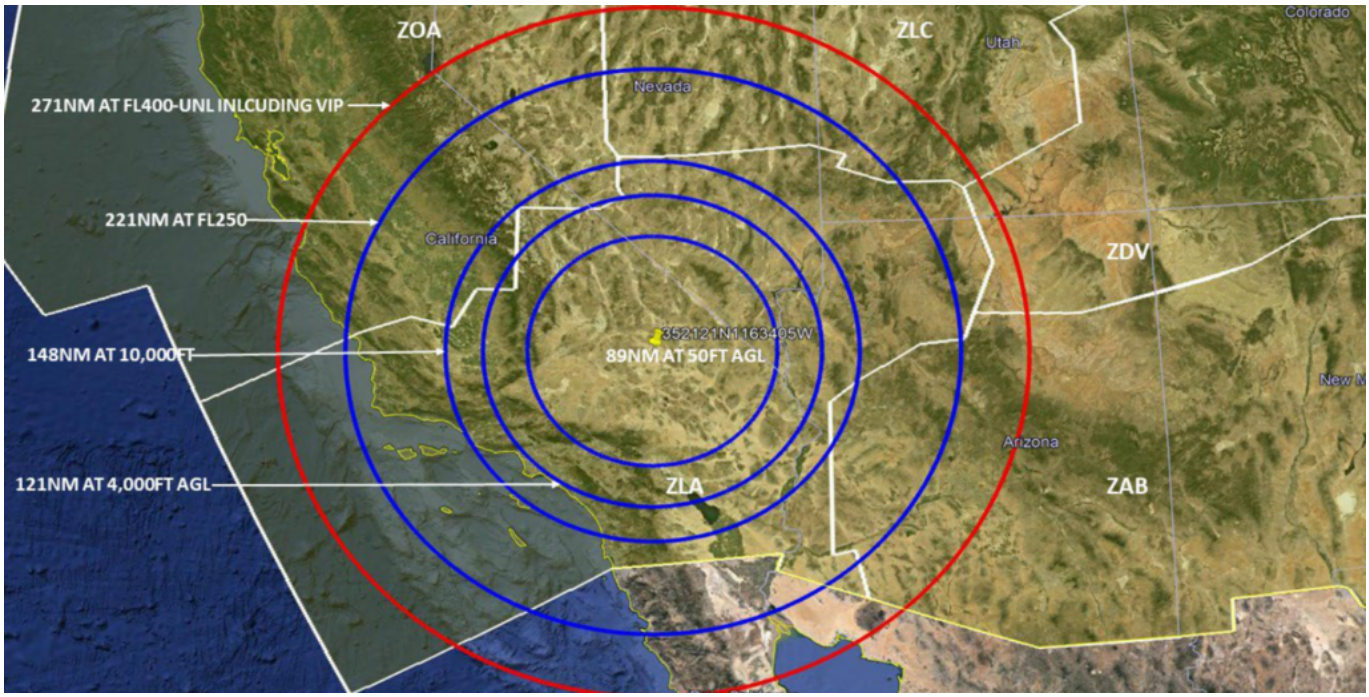
**20 March** 1830z – 2200z

**21 March** 0700z – 1259z  1830z – 2200z

**22 March** 1830z – 2200z

……..*(Local time GMT-7)*

Here's a map of the affected area:



*California Courtesy: FAA*

Testing will also be carried out up North at Ft. Greely in South-eastern Alaska across multiple days:

**15 March** 0001z – 0300z  0900z – 1200z

**16 March** 0001z – 0600z  1700z – 2000z

**17 March** 1800z – 2300z

**18 March** 2200z – 2359z

**19 March** 1800z – 2300z

**20 March** 2200z – 2359z

**21 March** 1800z – 2300z

**22 March** 1000z – 1700z

**23 March** 2200z – 2359z

**24 March** 1800z – 2300z

**25 March** 2200z – 2359z

……..*(Local time GMT-8)*

Here’s a map of the affected area:

### Don’t forget to report any outages.

It is important that any GPS interference is reported to the FAA – even though the interference is deliberate. There’s a proper process to follow for that which you can find in the Aeronautical Information Manual (AIM).

The relevant bits are paragraphs 1-1-13 and 5-3-3. Here’s a link to that document.

**But in a nutshell, aircraft should notify ATC, use a different source of navigation and if necessary, request an amended clearance.** It would also be a good time to grab a pen and write down as many details as you can as they’ll want a whole bunch of information in your report to the FAA. This will need to be submitted when you’re back on good ol’ terra firma. Click the link to see just how much information they’re after.

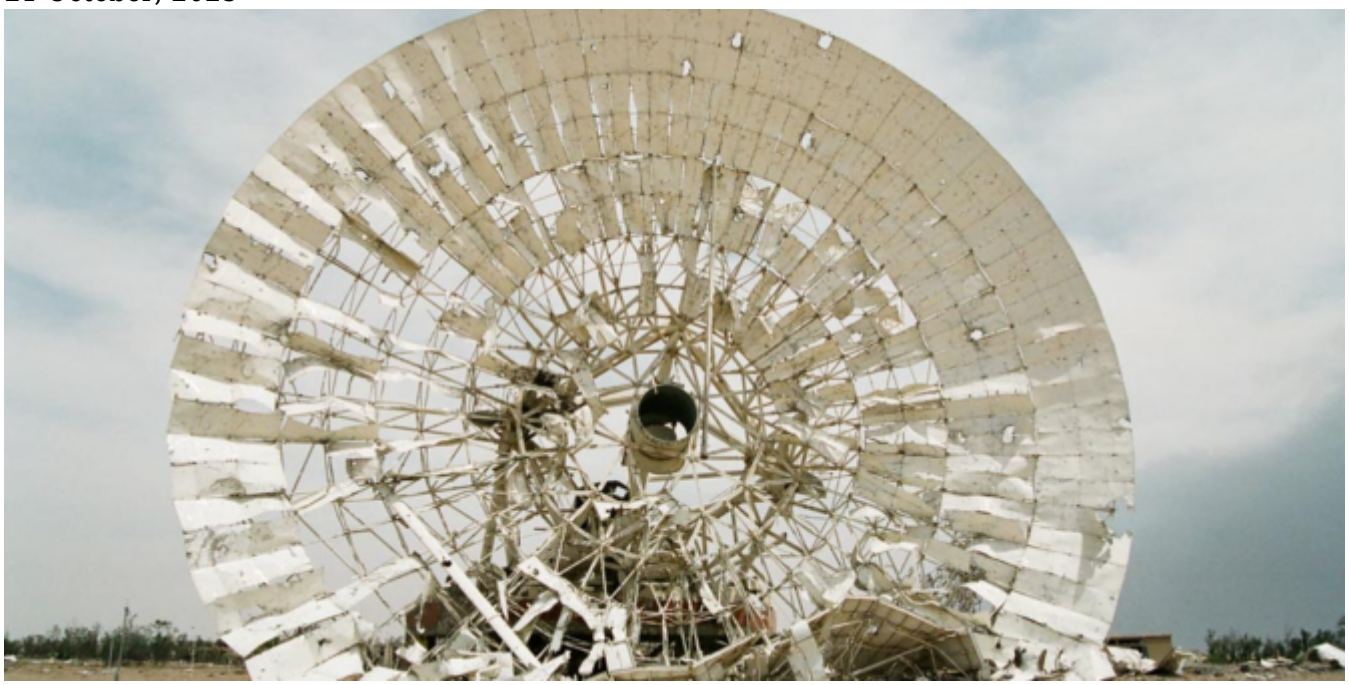
### Why should we bother reporting?

Because GPS jamming tests are an ongoing issue for civil aviation and it is important to keep tabs on just how much of a problem it is. They are having a growing impact on the US NAS which is becoming more and more dependent on GPS always being fully operational. Work is ongoing to safely accommodate these tests alongside aviation and the more info the industry has, the better.

---

# GPS U/S in the US

OPSGROUP Team
21 October, 2025



We have written a fair amount on worldwide GPS Jamming issues. Here is what we said about it in ‘GPS Jamming: All the Wrong Signals’. But there is another GPS problem though which is a little closer to home (if your ‘aviation’ home is in the US anyway).

### What's the deal?

Let's take a step back to 2017, when the NBAA and a bunch of other stakeholders took part in the 2017 RTCA tactical operation committee. That's the **Radio Technical Commission for Aeronautics** and they are great – they try and help find compromises amongst the competing interests on critical aviation modernization issues.

One of these very issues is with GPS.

The FAA's NextGen modernization program is using more and more GPS 'stuff'. Stuff that is critical for commercial flight operations safety and efficiency. The US Department of Defense on the other hand is sort of doing the opposite – they are running GPS Jamming tests which are critical for National Security and the **big problem** with this is that the jamming tests often interfere with the GPS signals civil aircraft are using.

### What was the 2017 outcome?

After they talked about it in 2017, the compromise was that the DoD will notify the FAA at least **120 hours before any planned tests.** This should give the FAA time or put out Notams to warn crew and operators.

### Problem solved?

Unfortunately not. The 120 hours notification is given, **but the information which filters down to the pilots and operators who need to know about it often not sufficient.** One of the difficulties is that the Notams have to provide information on different outage locations and this means **looooooooong Notams** filled with lots of Lat and Longs and times and dates. And this means critical information can sometimes get buried inside and makes it difficult or confusing for the crew to find it, extrapolate it (or even be aware of it in the first place).

### What's the plan now?

Well, the NBAA have reported on this, and say that the FAA are taking their concerns onboard. They plan to revisit the idea of producing **visual representations of the outage areas.** These will be much easier to digest than lines of lat and longs, and would hopefully enable crew to use them in conjunction with planning apps in the future.

There has also been a reminder issued to crew asking them to **report outages and issues.** If you find yourself in a jammy area, let ATC know. Tell them what you have lost so that they can warn other aircraft in the immediate area. The reminder has been sent to ATC as well because in the past, when aircraft have made these reports, the information has not always been shared out to other operators in the near vicinity.

### What do you need to look out for?

What an outage means, practically, is interference to the GPS signals which your navigation system is using. The result can be a **degradation in accuracy, or a full loss of the system** (GPS primary).

If you are enroute, let ATC know your capability has been degraded so you can get the support you need to continue navigating safely.

Some aircraft are particularly sensitive to disruption in the GPS signals, and it can lead to you losing that system until it is reset on the ground. **This means RNAV/RNP approaches might not be flyable anymore.** Having an awareness of what this means for your aircraft is important. Think about your plan B for approaches in case you do loose GPS navigation capability.

Notams are out there and it might be frustrating picking out the areas which could impact you, but

knowing about the outage spots in advance will help.

### Where can you look for info?

- The Navigation Center website is run by Homeland Security, and this is where you will find notices of GPS service interruptions and a link to their GPS Testing Notices. You can also file reports here if you encounter unexpected disruptions.
- This will take you to the Official government page on GPS.
- Your WAAS monitoring site is here. There are some good real time maps of current coverage
- The FAA also have a site where you can find Notams specific to GPS outages.

### The 5G Update

We thought we'd throw in a little update in on this as well.

Last year we saw increasing concerns about possible **interference from 5G networks** because they operate on the same slice of radio spectrum usually reserved for Radio Altimeter signals (the 3.7-3.98 GHz band).

The big concern here is that interference could result in degradation of accuracy from spurious emissions, or outright failures in the radio altimeters. Not sure how much of a risk that means? Well, Turkish Airlines TK1951 crashed in EHAM/Amsterdam Schiphol in 2009 and one of the primary factors was attributed to a malfunctioning radio altimeter which sent an erroneous -8ft reading to the autothrottle system, commanding it to idle.

**The NBAA are fronting a campaign here as well.** Twenty organizations have joined forces to send the FAA a letter raising their concerns over this, in response to a report issued on March 3 that they don't feel addresses the threat with enough analysis.

You can read the letter here.

Military aircraft and UAVs are also at risk here. Their radio altimeters use the same C-band frequencies, but they tend to fly a lot nearer the ground a lot more often. A very good summary of the issue can be found here.

---

# PBN, RNP and what it all means

OPSGROUP Team
21 October, 2025


All across Europe, 'Airspace Improvement Events' are occurring. It sounds huge. We were expecting new regions, routes, maybe some special-filtered cleaner air being puffed out into it…

Alas, we read through all the Airspace Improvement Event notices, and from what we gather, it is part of a big, ongoing project to implement things like **Free Route Airspace**, more **PBN routes**, and to basically **tidy up the airspace** a little. This is not limited to just Europe though – the world is going PBN.

### So, less an 'Event' and more a 'Something'?

Everything is moving to Performance Based Navigation. It has something to do with being compliant with EC Regulation 2018/1048, but really just comes down to more efficient, better, safer, increased capacity airspace and approach benefits for everyone.

As simply as possible – **VORs are out, Waypoints are in.**

In a bit more detail – fixed ATS routes will continue to be implemented for better flow management and lateral separation, you'll hear more about Free Route Space, and you'll start seeing more RNP approaches popping up at airports.

So it is actually quite a big change, but one that will be slow to get implemented. Actually, most countries brought in things like **RNAV5 routes** and **SIDs/STARs that use RNAV1 and GNSS** instead of old-fashioned, Navaid-based manoeuvrings quite some time ago, so this isn't something pilots will necessarily notice and there is no Big Date to look out for.

Except for one – **December 1 2022** (but we will get to that later).

### Why don't we like conventional Navaids anymore?

Well, old Navaids need a lot of maintenance and they break a lot. Ok, not a lot, but they do potentially **double the chance of some sort of issue** for an airplane relying on them. Take your bog standard ILS for example – it has ground transmitters and aircraft receivers (and all the bits around them and in between then) and if any one of these conks out then you can't fly the ILS (quite so well) anymore.

Your **GPS approach** on the other hand relies on the aircraft system only, which means less to go wrong.*

*Actually satellites can have issues too – GPS Jamming is a big problem and the plan to decommission

Navaids is being delayed because of this.

### So, what does this all actually mean, practically?

For operators, it doesn't mean a whole lot. Most aircraft will have been operating to RNAV5 for a fair old while now, so the only noticeable change will probably some **newly named waypoints**, and some **slightly more efficient routings**.

You might need to **pay a little more attention to any MELs** that affect your performance capabilities, and be aware that approaches might no longer have conventional Navaids as backups in the future because a bunch of these are getting decommissioned.

But overall, it really means keeping an eye on them charts to see what's happening where, and to make sure you pull the right plate out for your arrival.

### PBN, Say Again?

So, PBN, again. And December 1 2022. What happens then?

ICAO has ordered **all approach charts** to reflect the new specifications **by December 1, 2022.**

### What is changing?

All charts will say **RNP APCH** on them (or **RNP AR APCH**) instead of *RNAV, RNP (GNSS)* or whatever other random title they currently have. The chart should have the three lines of minima on it which you will need to know – your **LNAV**, **LNAV/VNAV** or your **LPV**.

### Which country is winning the chart race?

ICAO post updates on the implementation which you can follow here, although they last updated it in 2017 so let's hope it is looking a little better now.

### All the R's

In case you are still lost at RNP instead of RNAV, here is a quick recap on some terms for you:

- **GNSS** is your Global Navigation Satellite System and it is a generic terms for all satellite navigation systems including GPS, Galileo, GLONASS, and ones augmented by ABAS, SBAS, GBAS… all the BASes.
- **LNAV, VNVAV, LPV, LP** are your different minimus given on an RNP approach chart.
- **PBN** is Performance Based Navigation based on performance requirements of the aircraft on a route or approach or in designated airspace.
- **RNP** is required navigation performance which basically means the onboard monitoring and alerting system your aircraft has.
- **RNP Approach** is a generic term for any approach which uses GNSS to enable it and an RNP system to fly it.
- **RNAV Approach** is what RNP approaches used to be called.
- **RNP APCH** is the name of the navigation specification in the ICAO PBN manual for the 4 types of approach:
    - LNAV (GPS NPA)

    - LP (SBAS-based NPA)
    - LNAV/VNAV (APV Baro-VNAV)
    - LPV (APV SBAS or SBAS Cat I)

- **RNP AR APCH** is an approach the requires a specific aircraft qualification and operational approval. Usually because it takes places in an environment “rich in obstacles”. The AR stands for ‘approval required”. So you might be allowed to fly an RNP (RNAV) but not an RNP AR and your OpSpec (and training) are going to make this pretty clear.

### What is Free Route Airspace?

FRA is a specified volume of airspace in which users can freely plan a route between defined entry and exit points. It makes the sector much more efficient.

### And because we mentioned it earlier, what about RNAV?

Way back in the olden days (not as far back as when airplanes just had a compass and a map to use, but before GPS came in), there used to be Navaids. Ancient relics called VORs and NDBs which helped pilots work out where they were.

But then GPS came along and brought with it a way more effective and accurate way to navigate. How accurate is defined by ICAO under their four main navigation specifications – **RNAV10, RNAV5, RNAV2 and RNAV1**

**RNAV5** is actually fairly basic. It has been around in Europe since 1998 and is mandated in pretty much all high level airspace there.

The 5 bit refers to the requirement for aircraft to operate to a **minimum navigational accuracy of +/-5nm for 95%** of the time.

**RNAV1** is your precision RNAV (1 being +/-1nm). **RNAV10** is generally what you find over the oceans, and **RNAV2** is generally used in en-route areas of the US.

**Fun fact:** The UAE and Bahrain FIRs implemented RNAV1 a while back, which means you need GPS Primary to route into here. If you’ve encountered GPS jamming en-route, (common in Turkey, Iran, Iraq etc, read all about that here), then this might cause problems for you.

### What do you need for RNAV5 operations?

You need some sort of FMS, 1 IRS, 1 GPS or VOR/DME receiver and 2 nav displays.

### What about RNP?

If it is an RNP navigation specification then there is also a requirement for on-board performance monitoring and alerting. RNAV refers to ‘area navigation’ and it is slightly different to an RNP system (the monitoring and alerting requirements). PBN requires an RNAV or RNP system, while and RNP APCH specifically requires an RNP system.

### What else?

Actually, that’s about it. Except for the poor old UK that will no longer support LPV approaches from June.

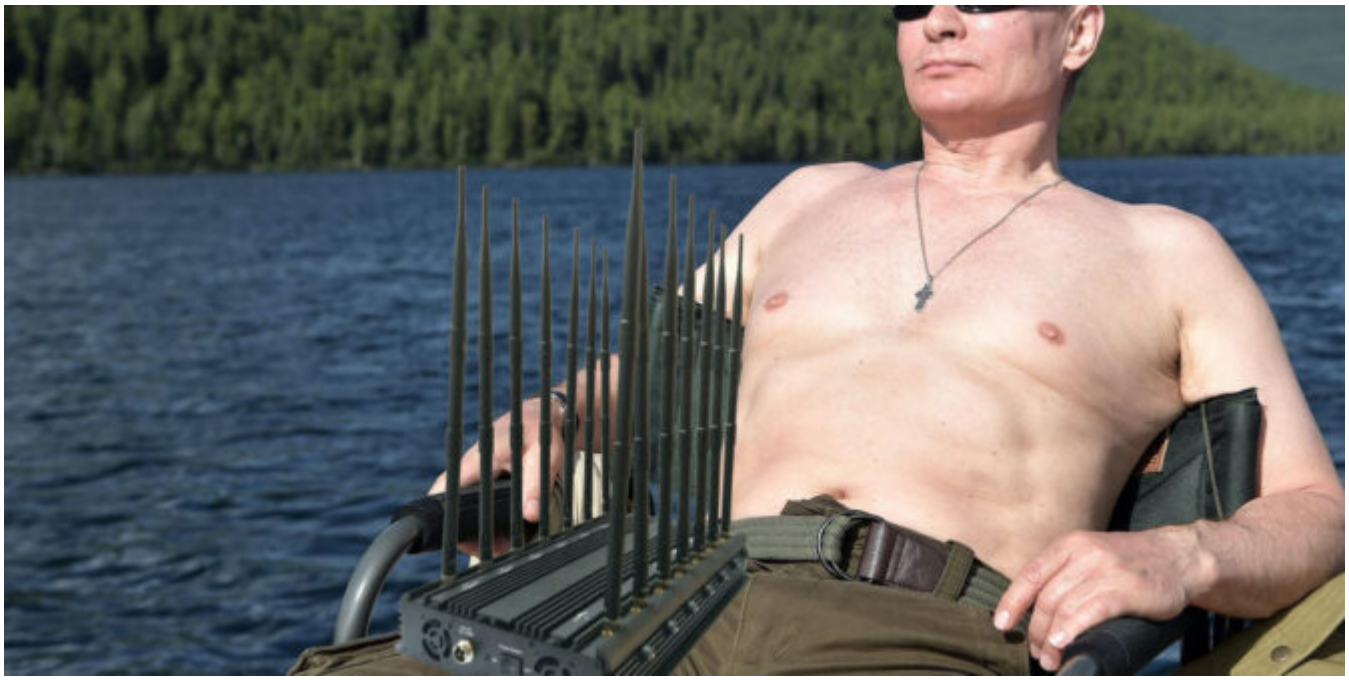
**Need to know more?**

Here is ICAO EUR Doc 025 which contains all the EUR RNP APCH Guidance Material.

---

# GPS Jamming: All the Wrong Signals

Chris Shieff
21 October, 2025



We live in a GPS world. This fantastic technology has **revolutionised aviation** since the first basic unit was approved for IFR use back in 1994.  It has become engrained in day to day operations. We use it for a bunch of really important stuff – navigation, communication, surveillance, ADS-B and even TAWS. It is a technology that we rely on to stay safe.

And herein lies the problem. It relies on radio signals from satellites to work, and they can be **intentionally interfered with**. If you operate between Europe and Asia then the chances are this is not new. What is concerning is that it is happening more and more. In the last five years EUROCONTROL report that cases of GPS outages have risen dramatically. The number one suspect? **Deliberate interference.**

### The Hot Spots

Almost always, widespread GPS outages occur in areas of political tension. It's no surprise then that the **Eastern Mediterranean, Middle East and Caucasus** are consistently the most affected regions – last year alone there were 3,500 reports of outages there. **About 10 a day**. And that's just from the people who spoke up. The **LCCC/Nicosia FIR over Cyprus** extending through to **LLBG/Tel Aviv** is particularly bad, with reports as far north as Italy, as well as **Turkey and Egypt.**

It is a part of the world **alive with tension** – spill over from the Syrian War, ongoing conflict in Libya and the current Azerbaijani conflict. Unfortunately it is also a **major air corridor** for flights between **Europe** and the **Middle East and Asia**. It is almost unavoidable.

But it's not just there – There are reports of GPS sabotage throughout the world – rings of interference

(also known as ‘crop circles’) have been traced to **China, North Korea** and even **the US**.

### So why tamper with GPS?

Unfortunately **electromagnetic warfare** is real. The goal for military interests is to make things as difficult as possible for the other side including disrupting communications and navigation. GPS jamming is also used as a defence against drones – the explosive ones which we see in the headlines, and the ones that are spying. In other cases, jamming is used to protect people’s **privacy**, and sometimes as a source of **criminal mischief.** Unfortunately for us, whether we like it or not, civil aviation is along for the ride…

### Jamming or Spoofing?

GPS signals are low power, which means that a **weak interference** source can cause a receiver to fail, or more concerningly **produce false information**. A basic way to achieve this is with jammers – devices that mask the signal with noise. Although they are illegal in the US, they’re not in other countries. And they’re readily available.

**A more sophisticated** approach used by the military is ‘**spoofing**’ where a ground station transmits a **fake GPS signal** that overrides the legitimate one.

In simpler terms – **jamming causes the receiver to die, spoofing causes it to lie.**

In powerful military applications, the effect of a single device has been known to affect a **300nm radius,** and it is almost impossible to locate them. They can be installed at bases, mounted in vehicles or put onboard ships.

### So why is this a problem for aviation?

**The issue is getting worse**, and outages are sporadic and unpredictable. Three quarters of GPS loss worldwide is occurring in the cruise, and in ten percent of these cases it lasts for **more than half an hour.** There have also been reports where GPS receivers never regained a signal. According to ICAO’s rules, frequent outages must be Notamed but the reality is, **few states are actually doing it.** To make matters worse, with so few aircraft flying during the pandemic it is unclear just how bad it is getting.

For crew, a loss of GPS forces an aircraft to rely on other means to navigate in airspace that **relies on accurate navigation** to separate you from other traffic. It can also lead to other issues including false alerts and even GPWS warnings. Requiring pilots to ignore them is a concerning precedent.

### The plot thickens, enter 5G.

We’ve all heard about it – the revolutionary technology that will let you download your favourite episode of ‘The Bachelor’ in record time. Worrying news in the US has emerged that the federal government has allowed a new network provider to access a slice of the radio spectrum **usually reserved for GPS signals** to power a huge 5G network across the country. The frequencies are powerful, and there is **no guarantee** that they won’t won’t interfere with GPS signals.

### So what can we do it about?

Unfortunately, like Covid, **the problem isn’t going away anytime soon.** While manufacturers work on new ways to protect your aircraft, there are a few things you can do.

The most important thing is contingency – **have a plan.** Be aware of the threat of jamming if flying in affected areas of the world, and the issues it may create for you in the flight deck. If you lose GPS signal, **report it to ATC.** The more reports they get, the better. They will work to increase your separation and coordinate with other units.

When you're flying a GPS-based approach, know what you'll do if the **screen goes blank**. Be prepared for the unexpected because as recent events have shown, that super reliable technology can fail.

And **stay informed**, here are some useful resources:

- EUROCONTROL – check out the latest stats on GPS outages here, and report loss of signal here.
- FAA – GPS Anomaly Reporting Form. For all US based GPS issues.

---

# Rockwell GPS fix coming soon

David Mumford
21 October, 2025

A large number of operators have been affected this week by a software glitch in some Rockwell Collins GPS receivers. After a few days of head-scratching, the cause of the problem was tracked back to the receivers' failure to compensate for the "leap second" event which happens once every 2.5 years when the US Government update their satellites – which they did on 9th June.

This meant that certain aircraft equipped with the affected GPS receivers suddenly started getting 'ADS-B fail' messages, which initially led to groundings of aircraft which did not have GPS on their minimum equipment lists (MEL).

In a note from Rockwell on Monday 10th June, they advise that the next scheduled update by the U.S. Government to the GPS constellation is set for Sunday 16th June at 0000Z. **This is when things should start working again, but they are not guaranteeing this will definitely fix the issue.** Rockwell told

OPSGROUP it's a **'wait and see'** situation.

In the meantime, it seems as though all the affected aircraft have been identified, and you should know at this stage if yours is working or not. Some aircraft remain grounded because there is no MEL relief. Rockwell are advising those who have not powered on their GPS units since the 9th June should leave them switched off. Make sure to check the advice from your OEM – some are advising to pull the GPS circuit breakers to prevent further issues.

Until the issue is fixed, many aircraft will be forced to fly non-RNP routes below FL280 and navigate VOR-VOR, or else remain on the ground.

For more on this, or if you have something to share, head over to the OPSGROUP forum.

---

# Europe squawks 7600 on ops in the Eastern Med

OPSGROUP Team
21 October, 2025

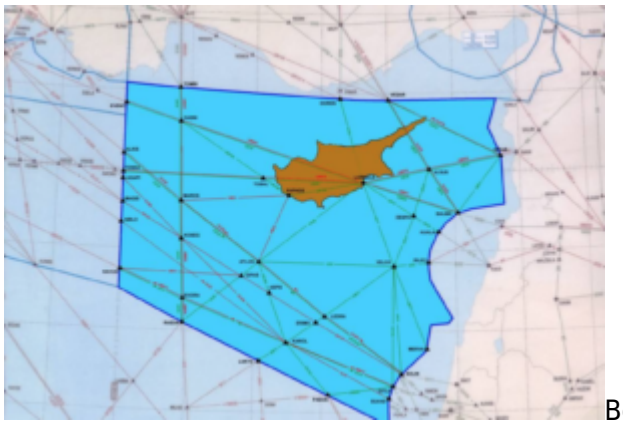

As we reported last month,  Eurocontrol published a 'Rapid Alert Notification' on their website regarding imminent air strikes into Syria.

> "Due to the possible launch of air strikes into Syria with air-to-ground and / or cruise missiles within the next 72 hours, and the possibility of intermittent disruption of radio navigation

> equipment, due consideration needs to be taken when planning flight operations in the Eastern Mediterranean / Nicosia FIR area.”

Around this time LCCC/Nicosia FIR released this vague (and now deleted) NOTAM:

> A0454/18 – INFORMATION TO AIRSPACE USERS
>
> THE DEPARTMENT OF CIVIL AVIATION OF THE REPUBLIC OF CYPRUS IS CONTINUOUSLY MONITORING THE GEOPOLITICAL DEVELOPMENTS IN THE REGION AND WILL NOTIFY THE AVIATION COMMUNITY IF AND WHEN ANY RELEVANT AN RELIABLE INFORMATION IS AVAILABLE THE DEPARTMENT OF CIVIL AVIATION IS TAKING ALL APPROPRIATE ACTION TO SAFEGUARD THE SAFETY OF FLIGHTS. 12 APR 15:25 2018 UNTIL 12 JUL 15:00 2018 ESTIMATED. CREATED: 12 APR 15:26 2018


Beyond this alert and NOTAM though; nothing else happened. A few days later, the conflict escalated.

Very few commercial flights operate over Syria, and authorities in the US, UK, France and Germany have all previously issued warnings for Syrian airspace.

But many airlines regularly transit the LCCC/Nicosia FIR: there are frequent holiday flights to the main Cypriot airports of LCLK/Larnaca and LCPH/Paphos; overflight traffic from Europe to the likes of OLBA/Beirut, OJAI/Amman and LLBG/Tel Aviv; as well as traffic from Istanbul heading south to the Gulf and beyond.

**What has happened in the few weeks since then?**

Normal Eurocontrol protocol is (during expected ATC strike for example) – regular teleconferences with operators, active re-routes and removal of certain overflight approval requirements. So did that happen this time? **No**.

Essentially just radio silence on Syria and operations in the Eastern Mediterranean Sea.

Right now, it's a busy place. With all the normal holiday traffic in the region, there is also a large number of military surveillance aircraft from numerous nations patrolling the region. United States assets operating from Greece and Italy. UK air power from Cyprus and the French from bases in Jordan. Add to that the normal Israeli defense air frames and even the odd Swedish gulfstream surveillance flight!  Then there are the Russians conducting aerial operations and defense exercises in and around Syria.

Cyprus has activated a litany of "temporary reserved/segregated areas" inside of Nicosia FIR.

On May 3rd, Cyprus issued this vague information, to 'exercise caution'.

> A0580/18 – NAVIGATIONAL WARNING TO ALL CONCERNED. EXTENSIVE MILITARY OPERATIONS IN NICOSIA FIR PILOTS TO **EXERCISE CAUTION** AND MAINTAIN CONTINUOUS RADIO CONTACT WITH NICOSIA ACC. 03 MAY 12:00 2018 UNTIL 31 MAY 23:59 2018. CREATED: 03 MAY 11:25 2018

There is also a current warning about GPS interruptions.

> A0356/18 – RECENTLY, GPS SIGNAL INTERRUPTIONS HAVE BEEN REPORTED BY THE PILOTS OF THE AIRCRAFT OPERATING WITHIN SOME PARTS OF NICOSIA FIR. AIRCRAFT OPERATORS OPERATING WITHIN NICOSIA FIR ARE ADVISED TO **EXERCISE CAUTION**. 20 MAR 10:04 2018 UNTIL PERM. CREATED: 20 MAR 10:05 2018

It may be unfair to blame the authorities completely. At the end of the day, due to the lack of appropriate communication from the various security agencies it's hard to get accurate information out there. Still, there was enough warning to alert civilian operators of imminent strike – but then nothing else. Shouldn't airspace customers and users expect more?

**So what to make of all this?**

Let's end it with this great 2009 (and still current) NOTAM from the Cypriots.

> A0687/09 – **NAVIGATION WARNING TO ALL CONCERNED.**
>
> 15 SEP 09:30 2009 UNTIL PERM. CREATED: 15 SEP 09:34 2009

---

# GPS Jamming at Cairo

Declan Selleck
21 October, 2025

Egypt notified airlines yesterday that GPS jamming is a concern to arrivals and overflights, and warned against conducting RNP/RNAV arrivals or approaches.

The jamming was announced on 24MAY, and is centred on Cairo Airport; the source is unknown.

Similar GPS jamming was conducted, at state level in that case, by North Korea last month, from five locations along the border with the South. South Korea, along with other Civil Aviation Authorities, are looking at an eLORAN based alternative as a backup.

Operators planning flights through the Cairo FIR should monitor NOTAMs for latest.