# Delhi GPS Interference: New Pilot Reporting Procedure

Chris Shieff
19 November, 2025

India's DGCA has issued **new pilot reporting rules** after a week of **GPS interference in the Delhi area.**

In early November, crews approaching VIDP/Delhi saw navigation anomalies including false EGPWS warnings, incorrect position data and altitude errors – **consistent with GPS spoofing.**

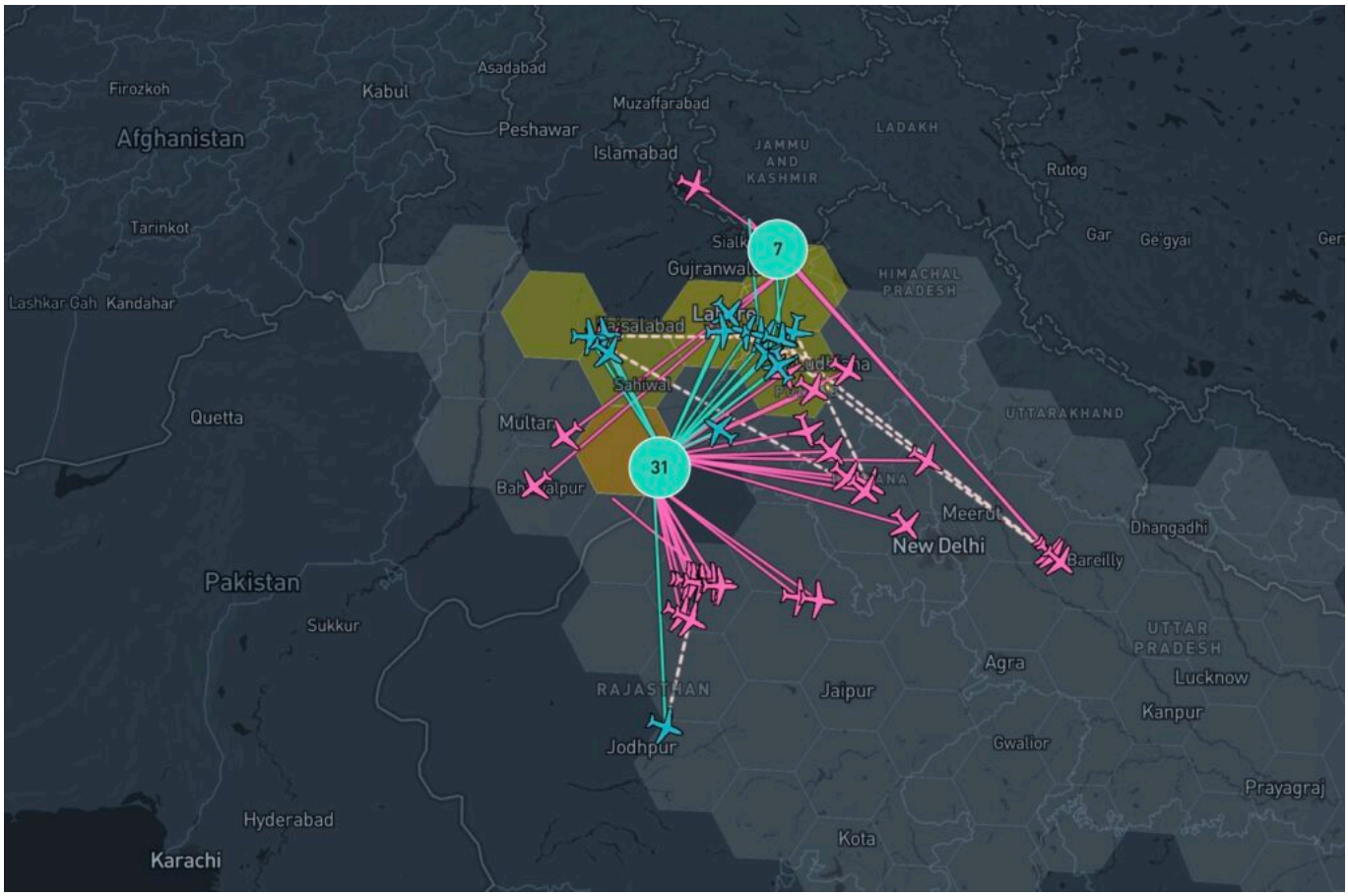



Image the work of GPSwise and SkAI Data Services.

Hundreds of flights were affected. ADS-B integrity in the Delhi TMA briefly dropped to zero, **leaving ATC unable to rely on GPS-based surveillance.**

The timing coincided with the **temporary withdrawal of ILS for runway 10/28**, which increased reliance on RNAV procedures.

### The paperwork trail

DGCA first outlined its GNSS-interference reporting process in a 2023 Advisory Circular.

On 10 Nov 2025, they followed up with a new SOP on GNSS Spoofing – which included the **"report within**

**10 minutes" requirement.**

Crews flagged parts of it as unclear, so on Nov 17, DGCA issued an Addendum to clarify exactly what pilots and operators must do!

## What pilots need to do

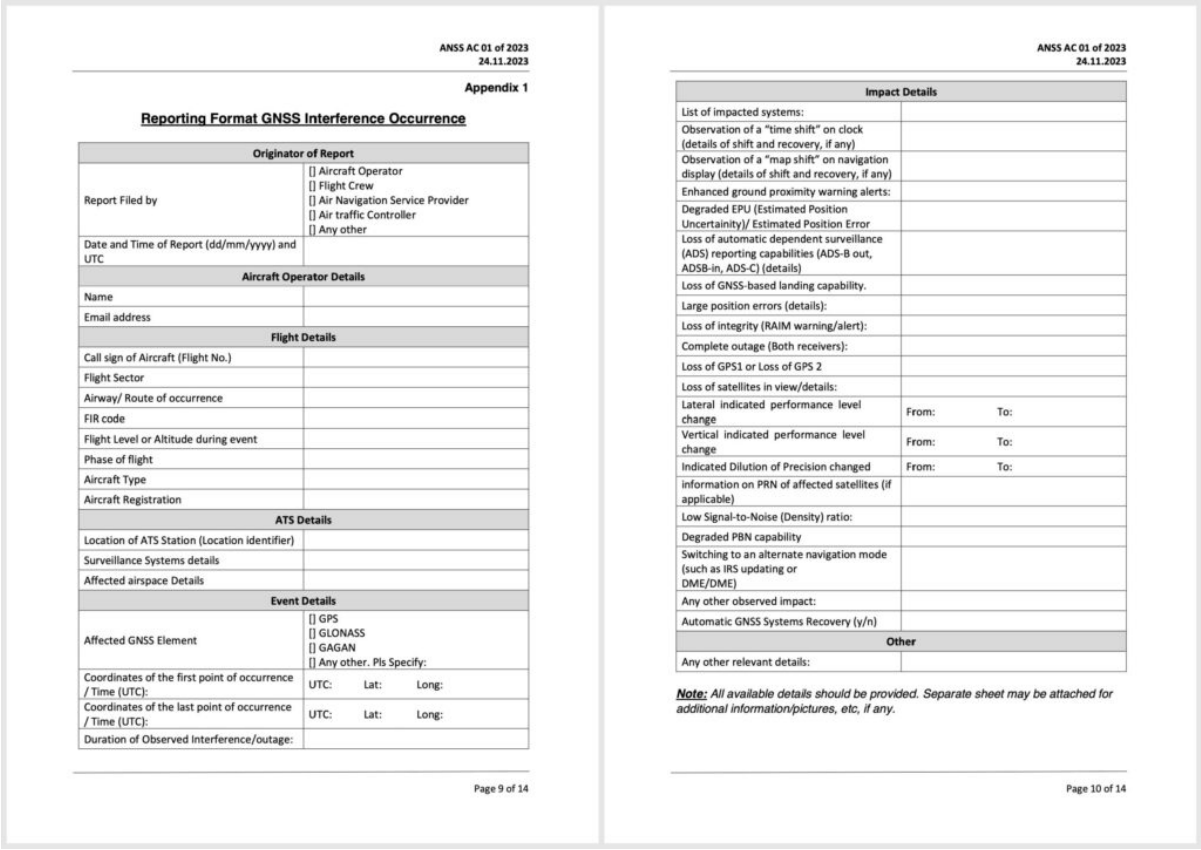
**If interference is detected <u>before</u> top of descent:**

1. Tell ATC as soon as possible.
2. Notify your operator's post holder (responsible manager) by any available means.
3. The post holder must then notify DGCA immediately using the form below.

**If interference is detected <u>after</u> top of descent, or only discovered <u>after</u> landing:**

1. Report it to the post holder as part of normal post-flight duties.
2. The post holder must then notify DGCA using the same form.

DGCA emphasises that the goal is timely reporting, not enforcement!



ANSS AC 01 of 2023
24.11.2023

Appendix 1

**Reporting Format GNSS Interference Occurrence**

| | |
|---|---|
| **Originator of Report** | |
| Report Filed by | [] Aircraft Operator<br>[] Flight Crew<br>[] Air Navigation Service Provider<br>[] Air traffic Controller<br>[] Any other |
| Date and Time of Report (dd/mm/yyyy) and UTC | |
| **Aircraft Operator Details** | |
| Name | |
| Email address | |
| **Flight Details** | |
| Call sign of Aircraft (Flight No.) | |
| Flight Sector | |
| Airway/ Route of occurrence | |
| FIR code | |
| Flight Level or Altitude during event | |
| Phase of flight | |
| Aircraft Type | |
| Aircraft Registration | |
| **ATS Details** | |
| Location of ATS Station (Location identifier) | |
| Surveillance Systems details | |
| Affected airspace Details | |
| **Event Details** | |
| Affected GNSS Element | [] GPS<br>[] GLONASS<br>[] GAGAN<br>[] Any other. Pls Specify: |
| Coordinates of the first point of occurrence / Time (UTC): | UTC: Lat: Long: |
| Coordinates of the last point of occurrence / Time (UTC): | UTC: Lat: Long: |
| Duration of Observed Interference/outage: | |

Page 9 of 14

ANSS AC 01 of 2023
24.11.2023

| | |
|---|---|
| **Impact Details** | |
| List of impacted systems: | |
| Observation of a "time shift" on clock (details of shift and recovery, if any) | |
| Observation of a "map shift" on navigation display (details of shift and recovery, if any) | |
| Enhanced ground proximity warning alerts: | |
| Degraded EPU (Estimated Position Uncertainity)/ Estimated Position Error | |
| Loss of automatic dependent surveillance (ADS) reporting capabilities (ADS-B out, ADSB-in, ADS-C) (details) | |
| Loss of GNSS-based landing capability. | |
| Large position errors (details): | |
| Loss of integrity (RAIM warning/alert): | |
| Complete outage (Both receivers): | |
| Loss of GPS1 or Loss of GPS 2 | |
| Loss of satellites in view/details: | |
| Lateral indicated performance level change | From: To: |
| Vertical indicated performance level change | From: To: |
| Indicated Dilution of Precision changed | From: To: |
| information on PRN of affected satellites (if applicable) | |
| Low Signal-to-Noise (Density) ratio: | |
| Degraded PBN capability | |
| Switching to an alternate navigation mode (such as IRS updating or DME/DME) | |
| Any other observed impact: | |
| Automatic GNSS Systems Recovery (y/n) | |
| **Other** | |
| Any other relevant details: | |

***Note:*** *All available details should be provided. Separate sheet may be attached for additional information/pictures, etc, if any.*

Page 10 of 14

Click for PDF.

## What to expect

A reminder that GPSwise (powered by the experts at SkAI Data Services) provides a **real time GPS**

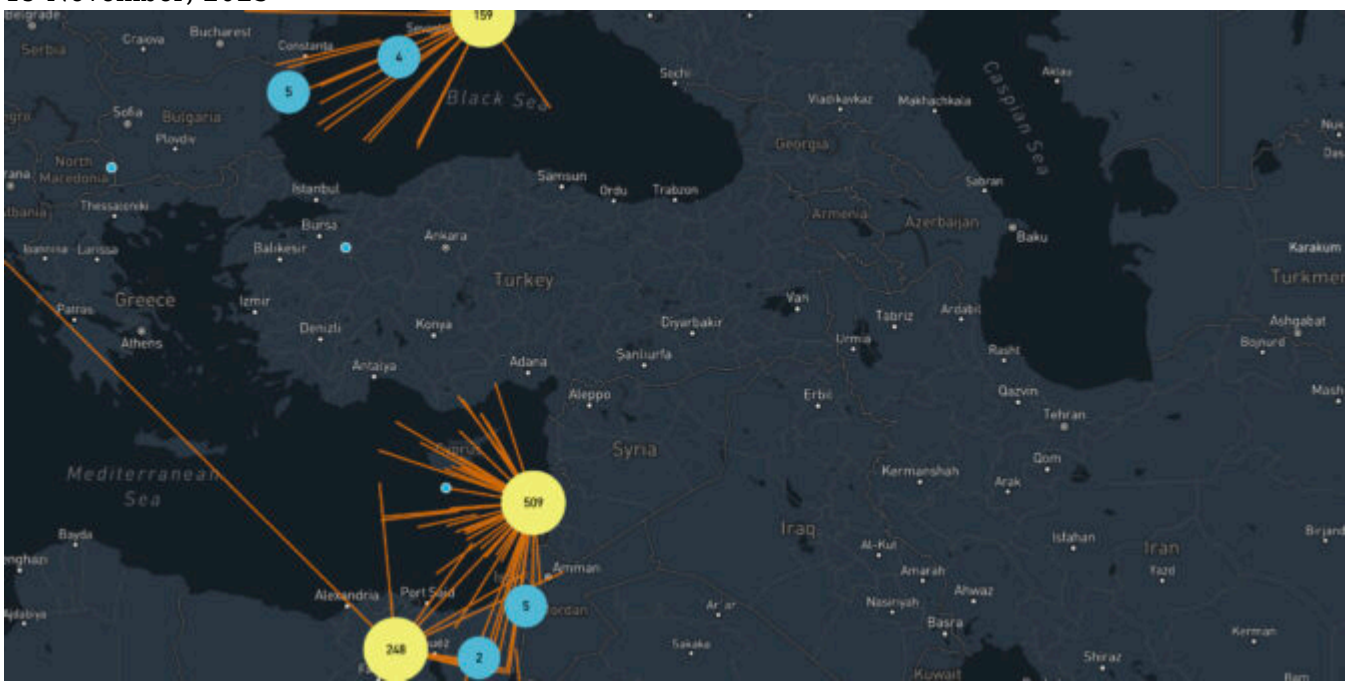
**Spoofing and Jamming map** spanning the globe. You can access it here.

Their current data shows a steady interference patch northwest of Delhi. It isn't constant, but it's there often enough that **crews should expect occasional GNSS issues** when routing through that area and be ready to cross-check and revert to conventional procedures.

---

# Where is the spoofing today? Two maps to help

Mark Zee
19 November, 2025

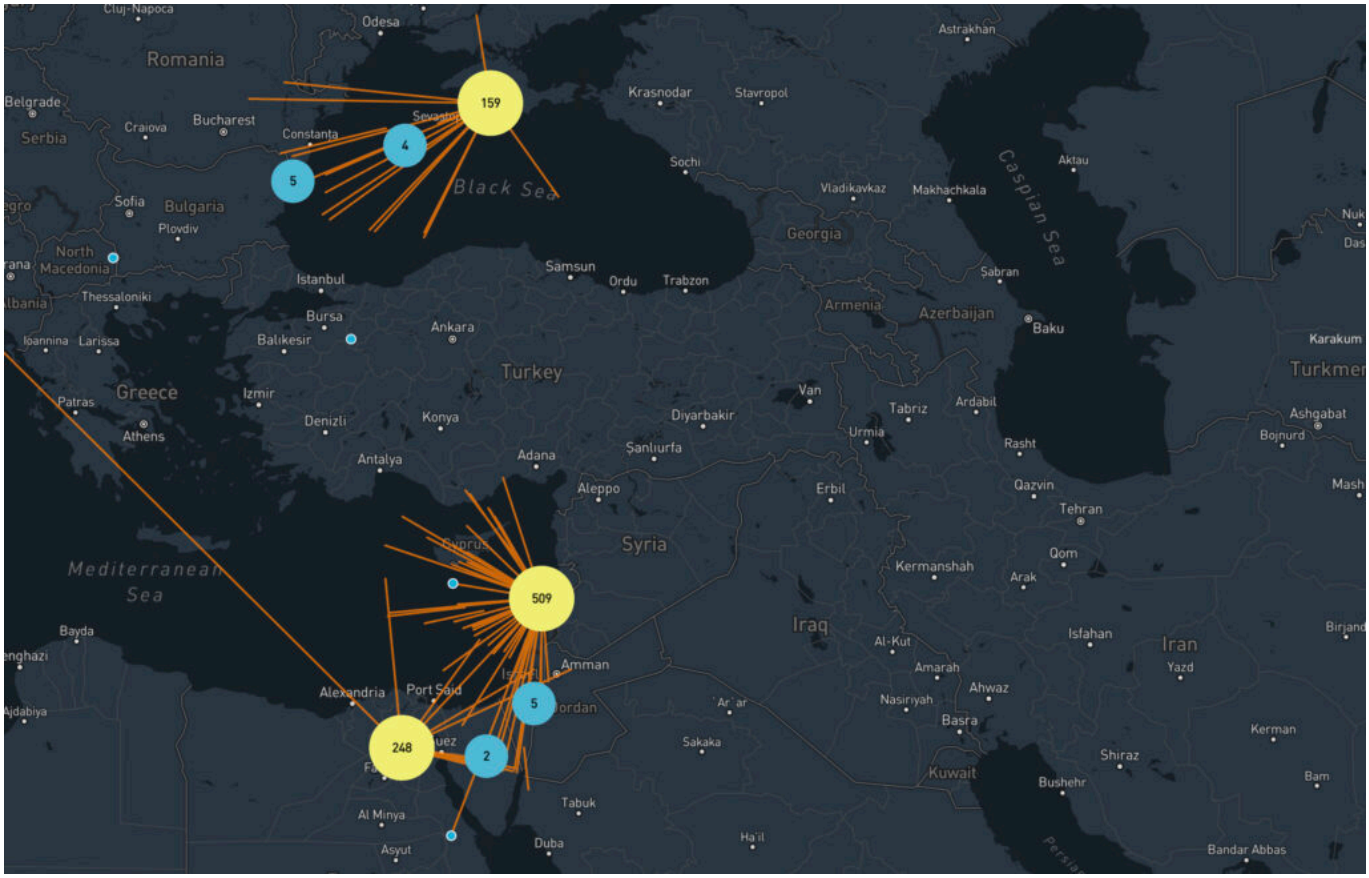



If you're keen to know exactly where GPS Spoofing – or GPS Jamming – might be happening today, there are two handy live maps to share with you.

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



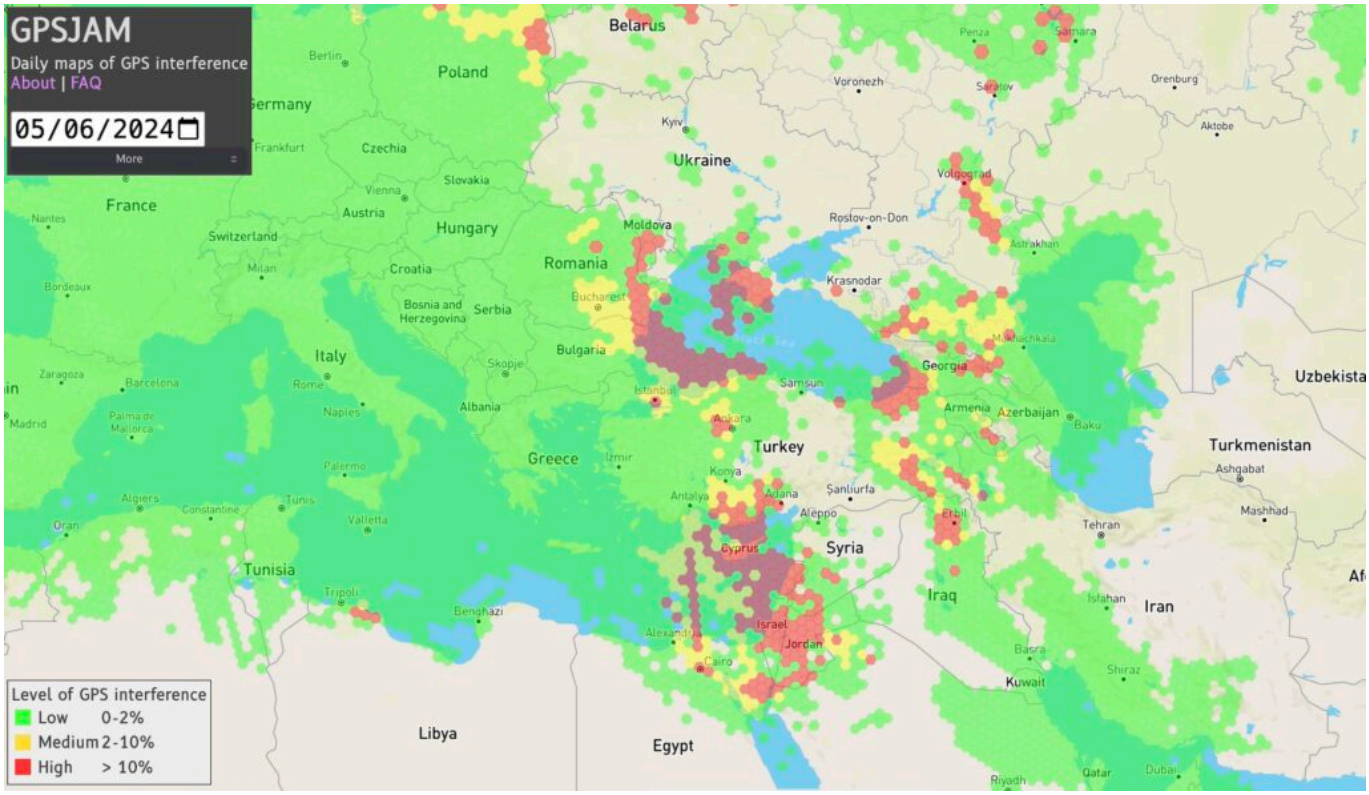

First up is this live **GPS spoofing tracker** from SkAI Data Services, in partnership with the Zurich University of Applied Sciences.

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.

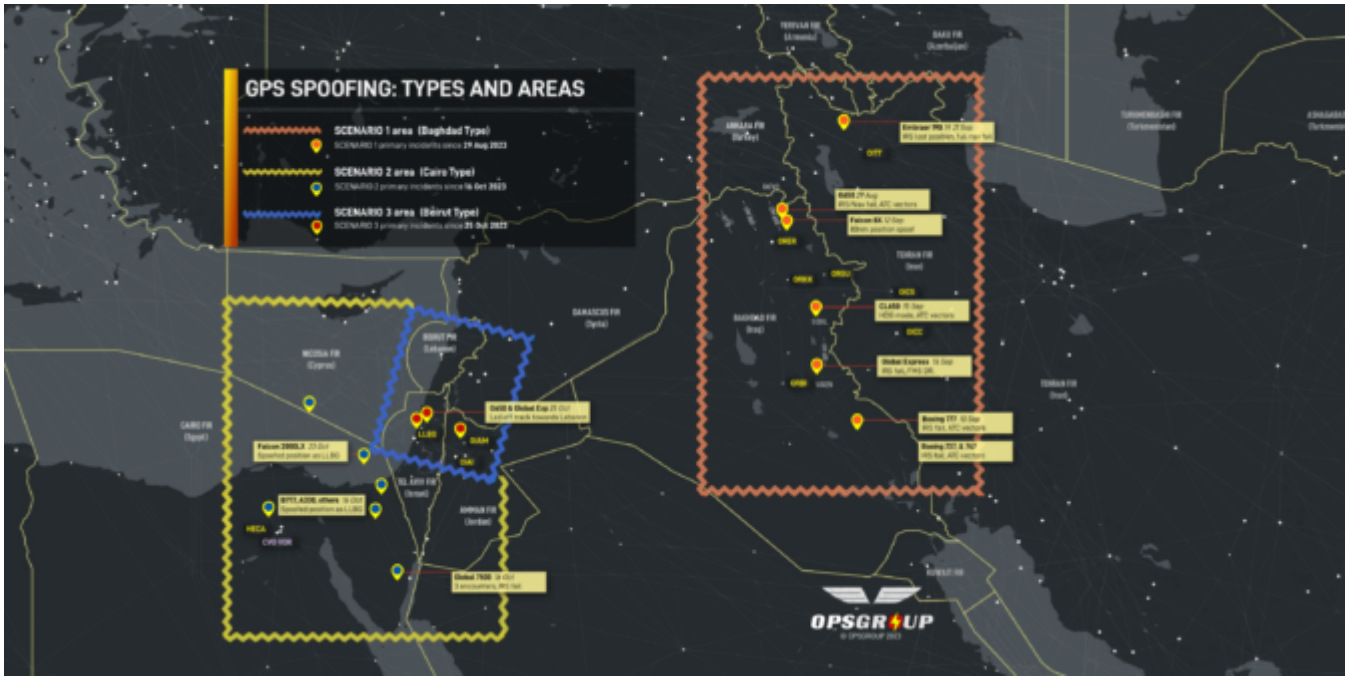
We continue to ask members to report GPS spoofing events (pictures are very useful too) to us at team@ops.group, or via WhatsApp to +1 747 200 1993. Thank you!

---

# GPS Spoofing Update: Map, Scenarios and

# Guidance

Mark Zee
19 November, 2025




**Key points in this update**

- **Two new types of GPS spoofing being reported, one leading to new critical nav failures**
- **Three distinct scenarios (Baghdad, Cairo, and Beirut types) – Spoofing Map published**
- **ALL CALL summary available in your Dashboard**

It's been 5 weeks since the real-world discovery of a **fundamental flaw in avionics design**: If a GPS position signal is faked, most aircraft are incapable of detecting the ruse. For many, it has lead to total navigation failure. For others, it has led to subtle and undetected erroneous tracking.

In the worst cases, the impact has been severe: complete loss of on-board nav requiring ATC vectors, IRS failure, and unnoticed off-track navigation towards danger areas and hostile airspace. The industry has been slow to come to terms with the issue, leaving flight crews alone to find ways of detecting and mitigating GPS spoofing.

**Two entirely new types of GPS spoofing** have been reported in other areas since the first GPS Spoofing **report** we published on 26 September. These include **critical nav failures on departure from Tel Aviv leading aircraft towards Lebanon**, and spoofed signals received by multiple aircraft in the **Cairo FIR** showing a stationary position over LLBG. We have now identified three distinct spoofing scenarios, shown on the map below and detailed in this briefing.

On Friday last, we asked OPSGROUP members for a group **ALL CALL** to gather the latest intel that we have in the community. This article will summarize at high level what we know. Full details are in your members dashboard (Special Briefings section).

***Note:*** This summary article is being continuously updated as we get more information. If you have anything to add or comment on, please **email the team**.

### Three scenarios: different types of spoofing

The GPS Spoofing reports received by OPSGROUP can be divided into three main scenarios, which correspond to the areas on the map below.

### Key Flight Crew concerns

- **Uncertainty** as to the best way to mitigate GPS spoofing activity
- Wide concern over **IRS spoofing**, previously thought to be impossible
- Potential for the issue to recur in other geographic areas
- Potential for **surprise and startle effect** with sudden loss of nav capability
- **Lack of useful guidance** from aviation authorities, OEM's and avionics manufacturers

### Worst case reports

In all, OPSGROUP has received close to 50 reports of GPS spoofing activity. Further down, we identify **three distinct spoofing scenarios** reported by flight crew. First, we highlight the most troubling reports to show how critical the impact can be.

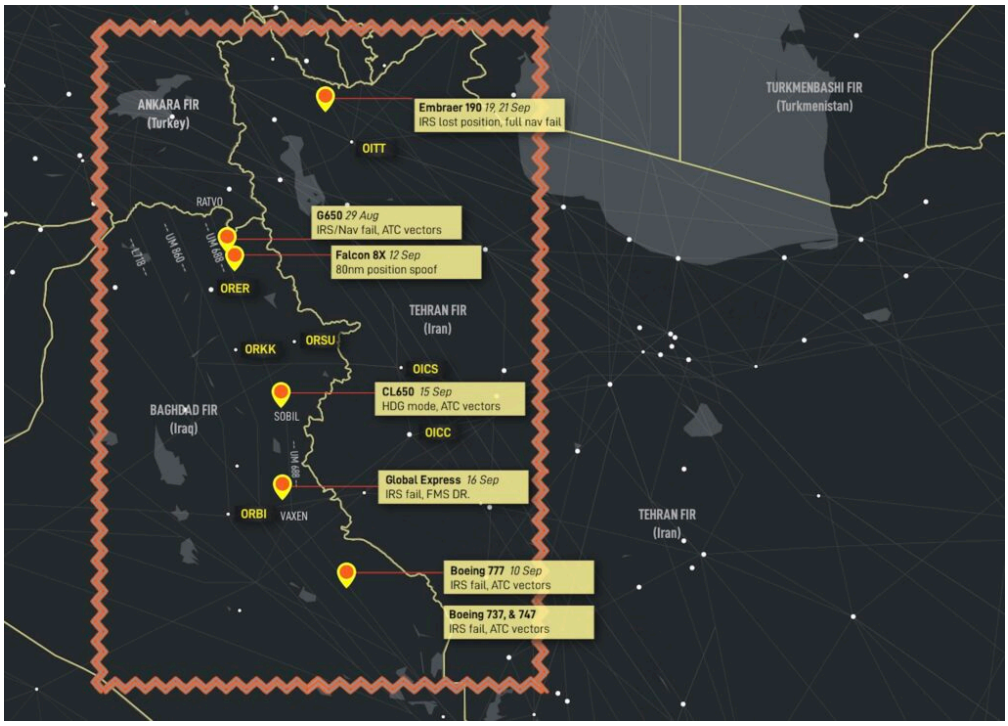
- A **Gulfstream G650 experienced full nav failure** on departure from LLBG/Tel Aviv (25 Oct). The crew reports, "ATC advised we were off course and provided vectors. Within a few minutes our EPU was 99.0, FMS, IRS, and GPS position were unreliable. The navigation system thought it was 225nm south of our present position." [Full report – Members Dashboard].
- A **Bombardier Global Express** was spoofed on departure from LLBG/Tel Aviv (16 Oct). A false GPS position showed position as overhead OLBA/Beirut. Crew advises "The controller warned us that we are flying towards a forbidden area". [Full report – Members Dashboard].
- A **Boeing 777** experienced a 30 minute GPS spoofing encounter in the Cairo FIR (16 Oct). A false GPS position showed the aircraft as stationary overhead LLBG for 30 minutes.
- A **Bombardier Global 7500** was spoofed 3 separate times in the Cairo FIR (16 Oct 2023). Crew advises: "The first took out one GPS, the second took out a GPS and all 3 IRS's, and the third time took both GPS's and all 3 IRS's." The distance from LLBG was roughly 220-250 miles, and the spoofing stopped once we were approx 250nm west of LLBG.
- An **Embraer Legacy 650** 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.**

- A **Bombardier Challenger 604** experienced spoofing in the Baghdad FIR and required vectors all the way to Doha. “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.

#### Scenario 1: Baghdad type.

**Affected area:** Primarily **Northern Baghdad FIR,** especially on airway UM688. Also, northern **Tehran FIR**, **Baku FIR**

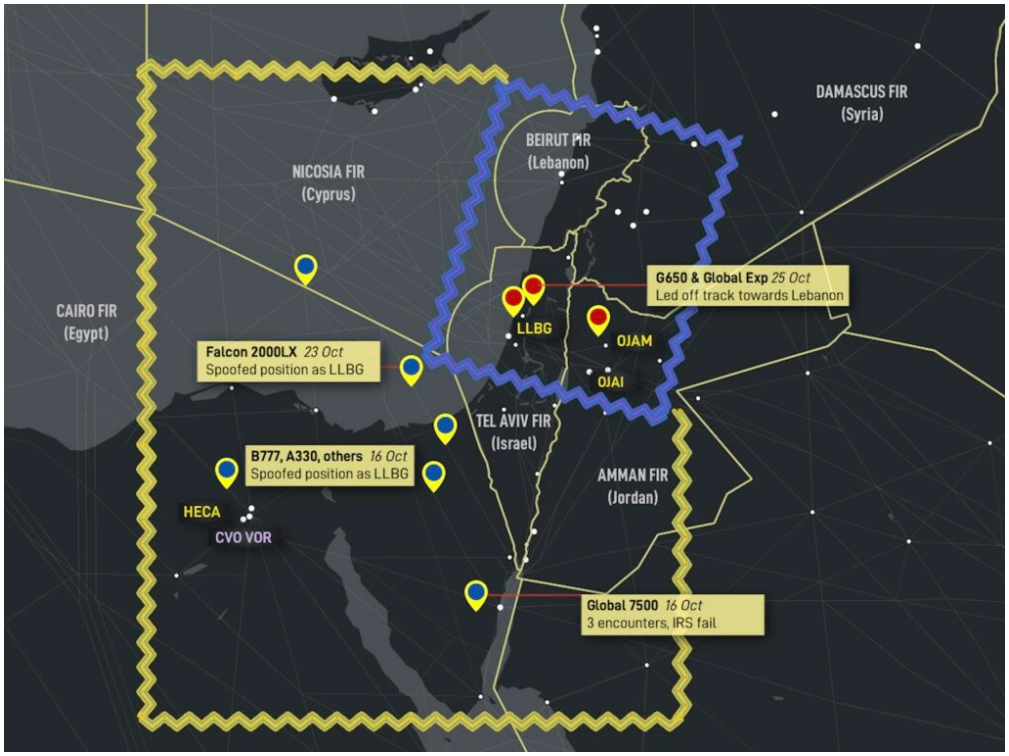



The **Baghdad** spoofing type involves GPS spoofing of enroute aircraft, nav failures follow. This was the first type of spoofing, initially reported on August 29, 2023, with a large amount of further reports starting in September 2023.

**Dashboard:** See full briefing on this type, with the original full crew reports.

#### Scenario 2: Cairo type

**Affected area:** Primarily within the **Cairo FIR** (L560, and locations near CVO VOR), also **Nicosia FIR** (Cyprus), **Amman FIR** (Jordan)

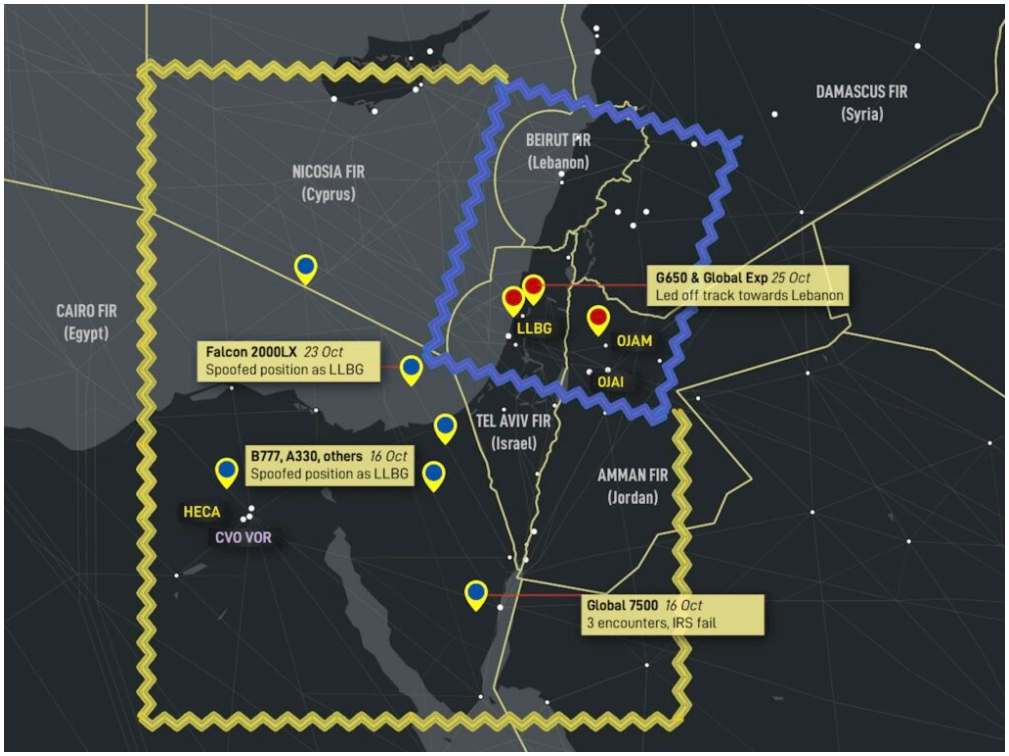



These reports first surfaced around Oct 16. Most reports are within the Cairo FIR. All crew reported similar circumstances, where a false or spoofed GPS position is received by the aircraft, incorrectly showing the aircraft position as being over LLBG/Tel Aviv. Locations vary from airways over the eastern Mediterranean, Egypt, and also on approach into Amman, Jordan (OJAM). Reports range from 100nm to as far as 212nm from LLBG.

**Dashboard:** See full briefing on this type, with the original full crew reports.

#### Scenario 3: Beirut type.

**Affected area:** Primarily within the **Tel Aviv FIR**, also **Nicosia FIR** (Cyprus), **Amman FIR** (Jordan)




Here, the spoofed position shows the aircraft over OLBA/Beirut, or creates subtle tracking towards OLBA. This type has been responsible for wayward tracking on SID departures from LLBG since October 25.

**Dashboard:** See full briefing on this type, with the original full crew reports.

## How to identify spoofing

The big question for flight crew is: how do I know this is happening to us? As always, **we are in the front line of dealing with this**. What will you do at 2am over the Middle East when the aircraft starts drifting off course and saying “Position Uncertain”? With almost zero guidance, we’re largely on our own to figure things out.

The following are based on the reports submitted to OPSGROUP by crews that have experienced spoofing:

1. **Sudden increase in EPU** (Estimated Position Uncertainty). GPS jamming will not create this, but a spoofed position will cause a “jump” and hence EPU values have jumped from 0.1nm to 60nm, and >99nm in quick order.
2. An **EFIS warning** relating to Nav. Some aircraft have gone straight to “DR” mode (Dead Reckoning).
3. A sudden large change in the aircraft clock UTC time. Reports vary from a couple of hours to 8 hour and 12 hour changes in the aircraft clock time.

Obviously, every aircraft has different system architecture and will behave differently, but these tell-tale indicators should help to identify the first signs of spoofing.

### Mitigation – BEFORE entering known areas

At base level, there is no effective way to prevent the actual GPS spoofing from happening. If it exists, a false signal will be received by the aircraft. As mentioned above, most aircraft are not able to understand that this is happening – there is no software logic that detects large sudden jumps in GPS position as being potentially false.

1. The critical first step is **knowing** when you are entering a potential GPS spoofing area (see locations above)
2. Consider **de-selecting GPS as a sensor input to the FMS** (to avoid nav uncertainty)
3. Consider, if possible, **de-selecting GPS updating to the IRS** (to avoid loss of IRS)
4. Monitor ATC for any other aircraft comments that indicate spoofing (time checks, position checks)
5. Identify conventional navaids that can be used instead (VOR, NDB)
6. **Departure** – there is uncertainty as to whether de-selecting GPS inputs on the ground before departure into known spoofing areas is sensible. Some OEM's have said this may lead to other issues.

**Mitigation – DURING active spoofing**

If you experience GPS spoofing

1. As soon as possible, de-select any GPS inputs (FMS, IRS). Crew reports suggest that **quick action here** (within 60 seconds) can prevent wider nav failure
2. Switch to using conventional navaids (VOR, NDB)
3. If you know that for your aircraft type the IRS is not capable of being spoofed, obviously IRS navigation is preferable for accuracy.
4. Report the occurance to ATC, primarily to warn other flight crew on the same frequency.

Please also **report** the occurance to OPSGROUP, to continue building a picture of where these events are occuring. All reports are anonymous and de-identified.

#### ALL CALL Summary – GPS Spoofing

An ALL CALL to the group pools our knowledge on particular topics. This ALL CALL went out on Nov 2. View the **original email**, or scroll to the end of this post. If you have anything to add, please email news@ops.group. As we get updates, we'll post them here.

**View the live-updates in the ALL CALL response here**.

- New crew GPS Spoofing reports following ALL CALL
- Member comments on GPS Spoofing
- **OEM guidance:** Dassault
- **OEM guidance:** Gulfstream
- **OEM guidance:** Boeing
- **OEM guidance:** Bombardier
- **OEM guidance:** Embraer
- Aviation Authority guidance (EASA)
- **Update on GPS issues in Shanwick OCA**

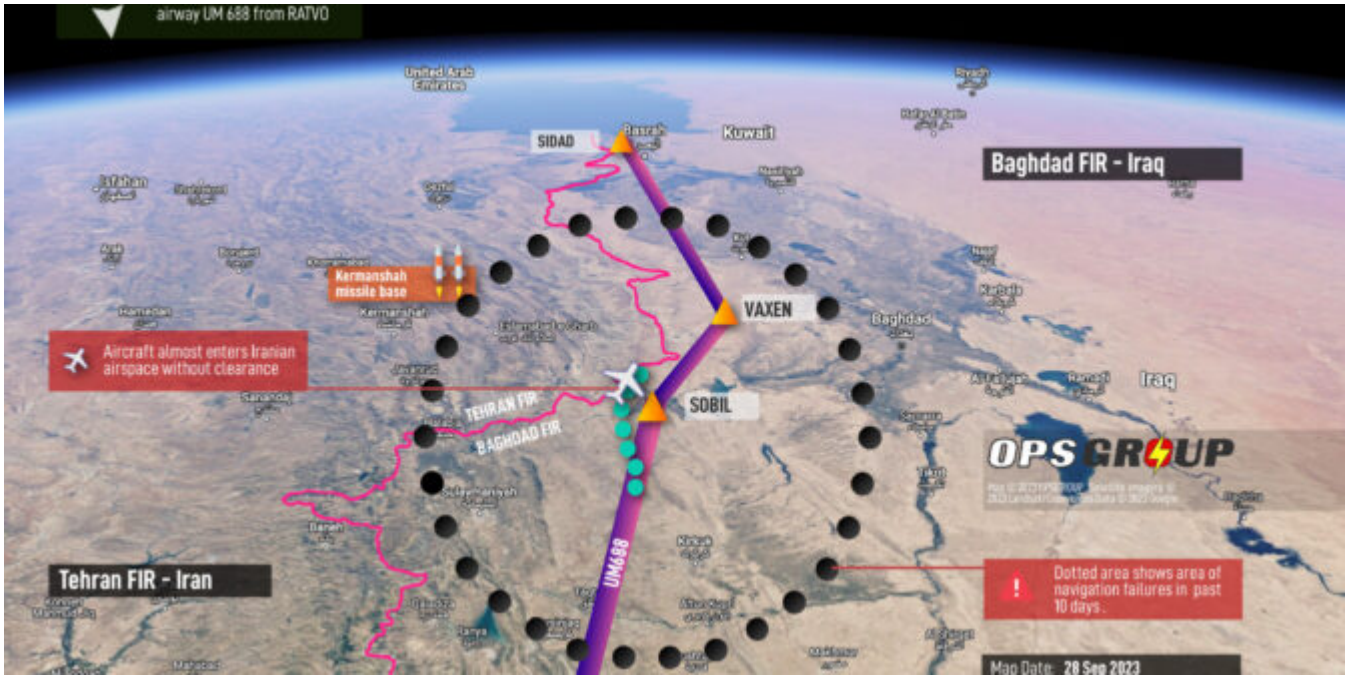
**Further reading**

- First report on GPS Spoofing, OPSGROUP – “Flights Misled over position, nav failure follows” (26 Sep 2023)
- Update, FAA warning, OPSGROUP – “FAA warning issued” (28 Sep 2023)
- **Download**: RISK WARNING (**V2/28SEP**) – **Fake GPS signal attacks** (PDF, 1.7 Mb)
- **Member Briefing**: GPS Spoofing, Nav Failures
- **Member Briefing**: GPS Spoofing Scenarios (Baghdad, Cairo, Beirut types)
- **Member ALL CALL summary**: GPS Spoofing 02 Nov. (Live updates)

---

# FAA warning issued, further serious navigation failures reported

OPSGROUP Team
19 November, 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.

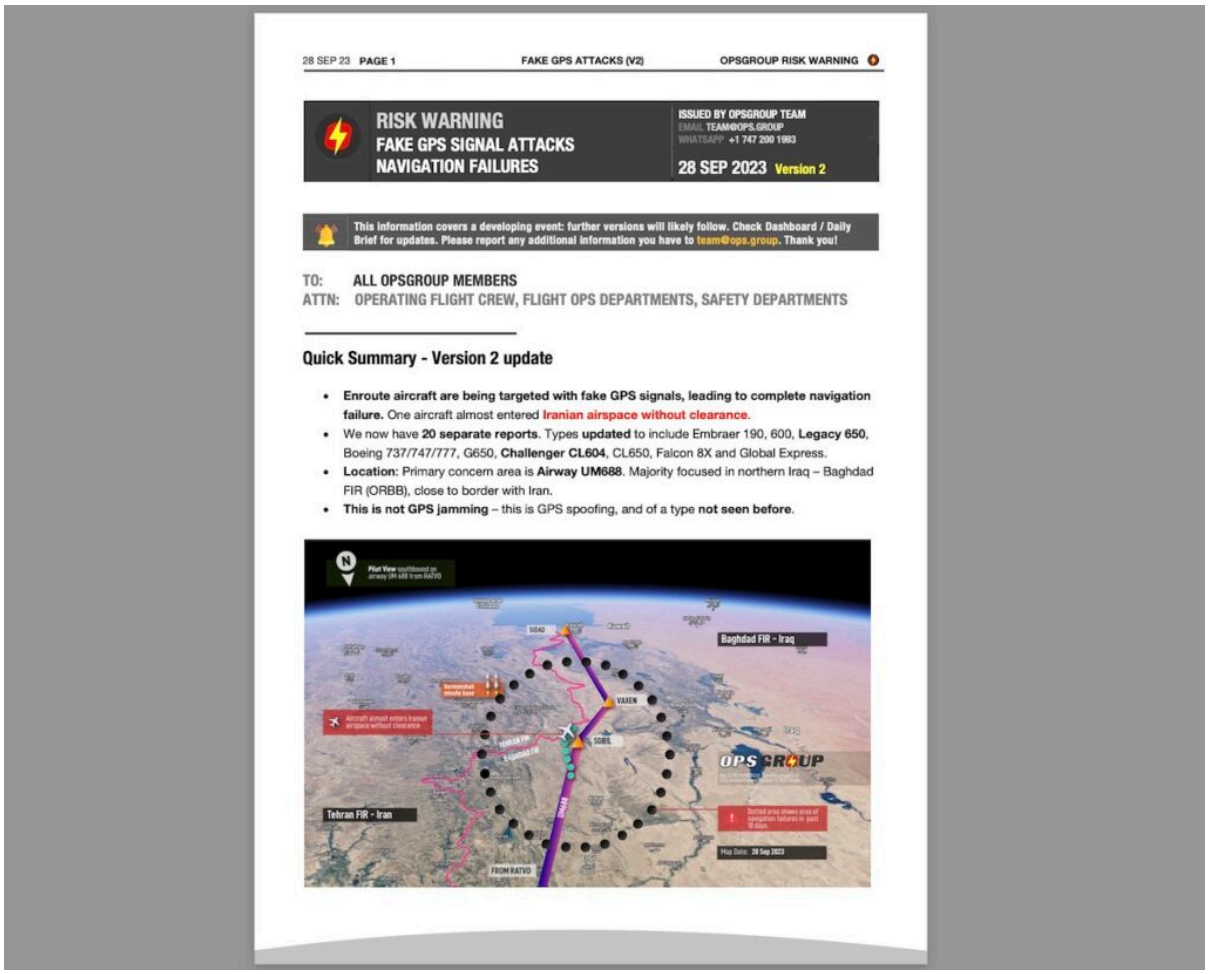
Exactly where the avionics problem arises as a result of these GPS spoofing signals is something that OEM’s and Avionics providers are working on. However, **many modern IRS platforms include GPS updating while enroute, to correct drift**.

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 1993
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!

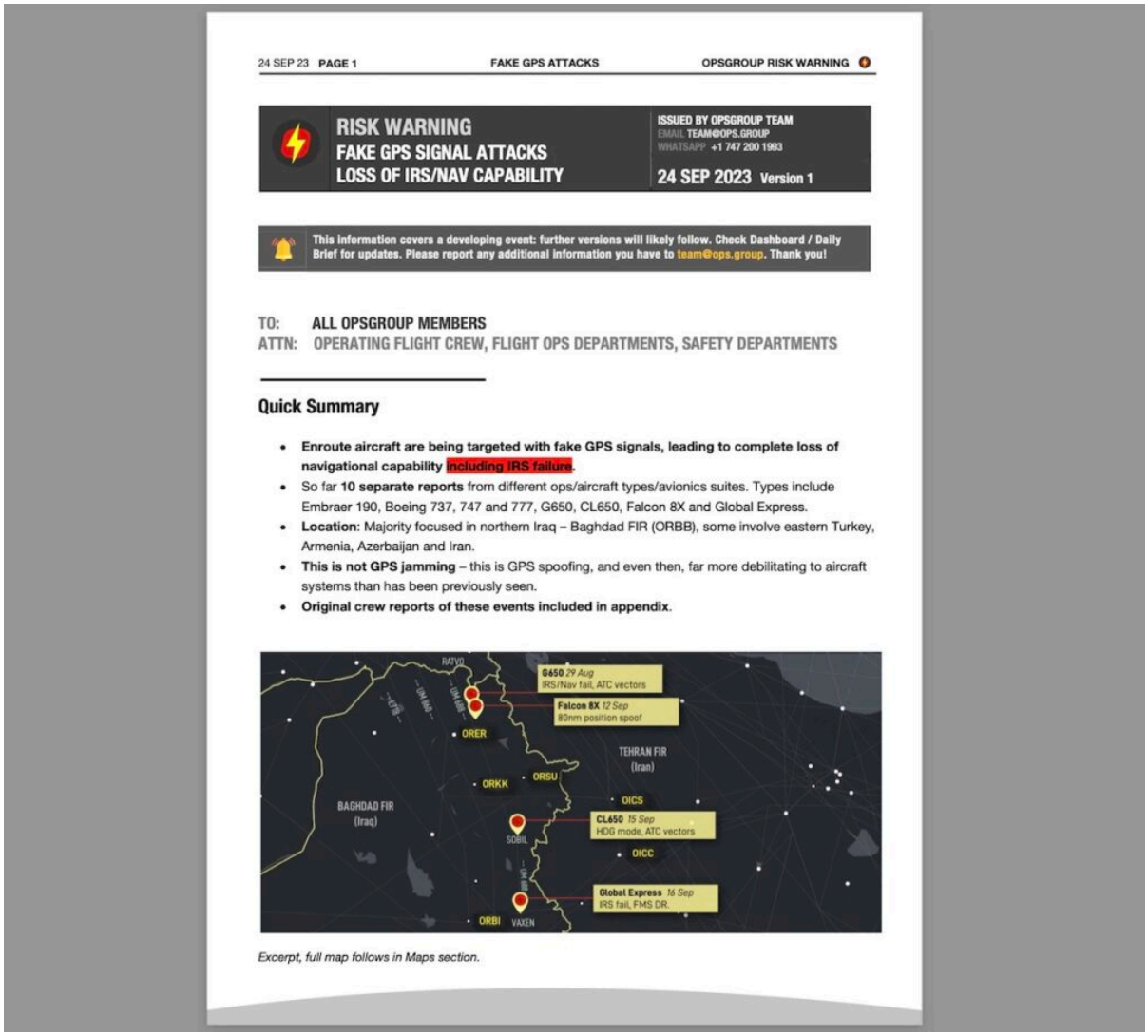
TO: ALL OPSGROUP MEMBERS
ATTN: OPERATING FLIGHT CREW, FLIGHT OPS DEPARTMENTS, SAFETY DEPARTMENTS

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
19 November, 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

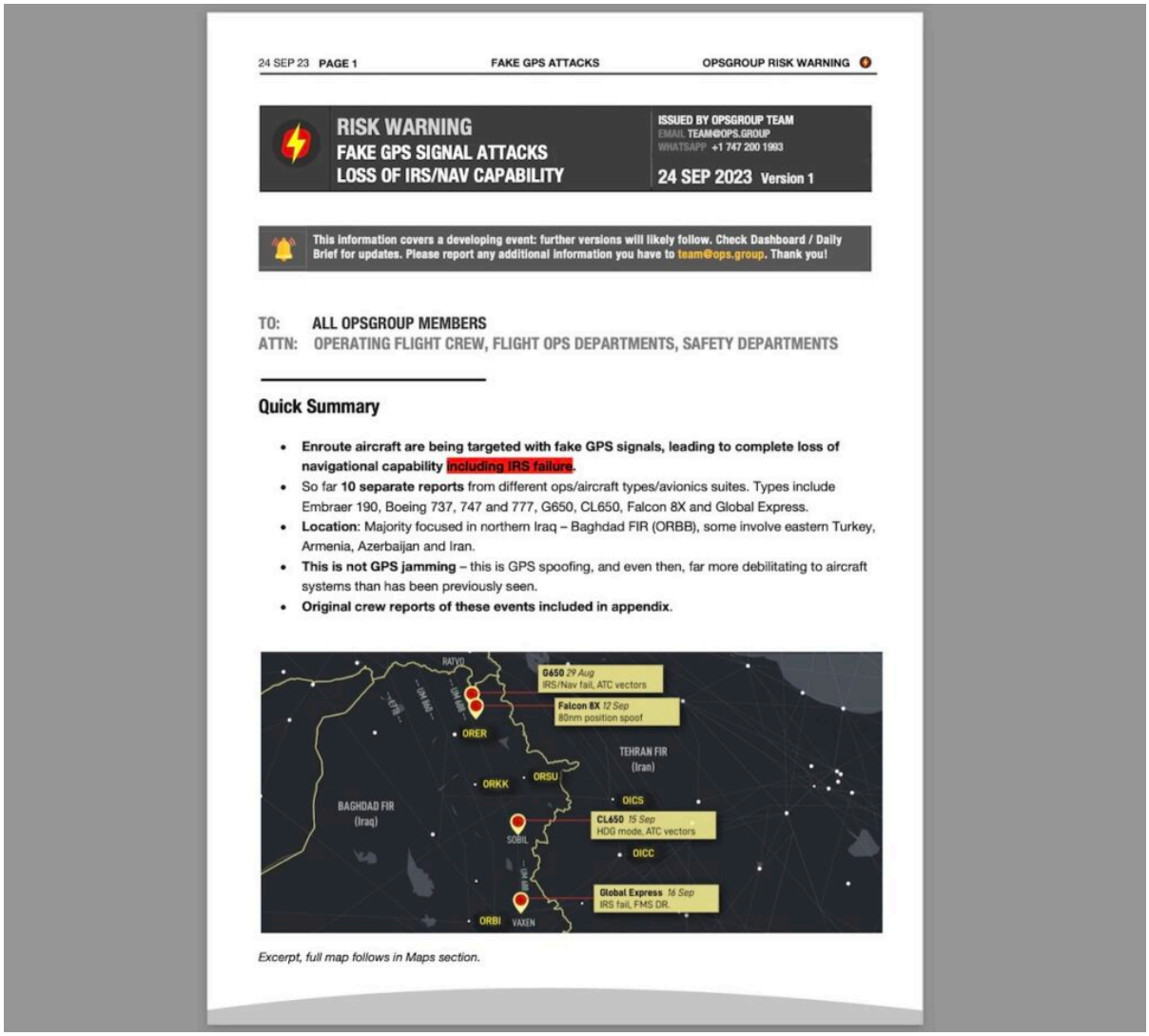
**along UM688**. This airway runs southbound through Iraq, **above an active conflict zone**, and extremely close to the border with Iran. Any indavertent straying into Iranian airspace without a flight plan risks action by the Iranian military.

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!