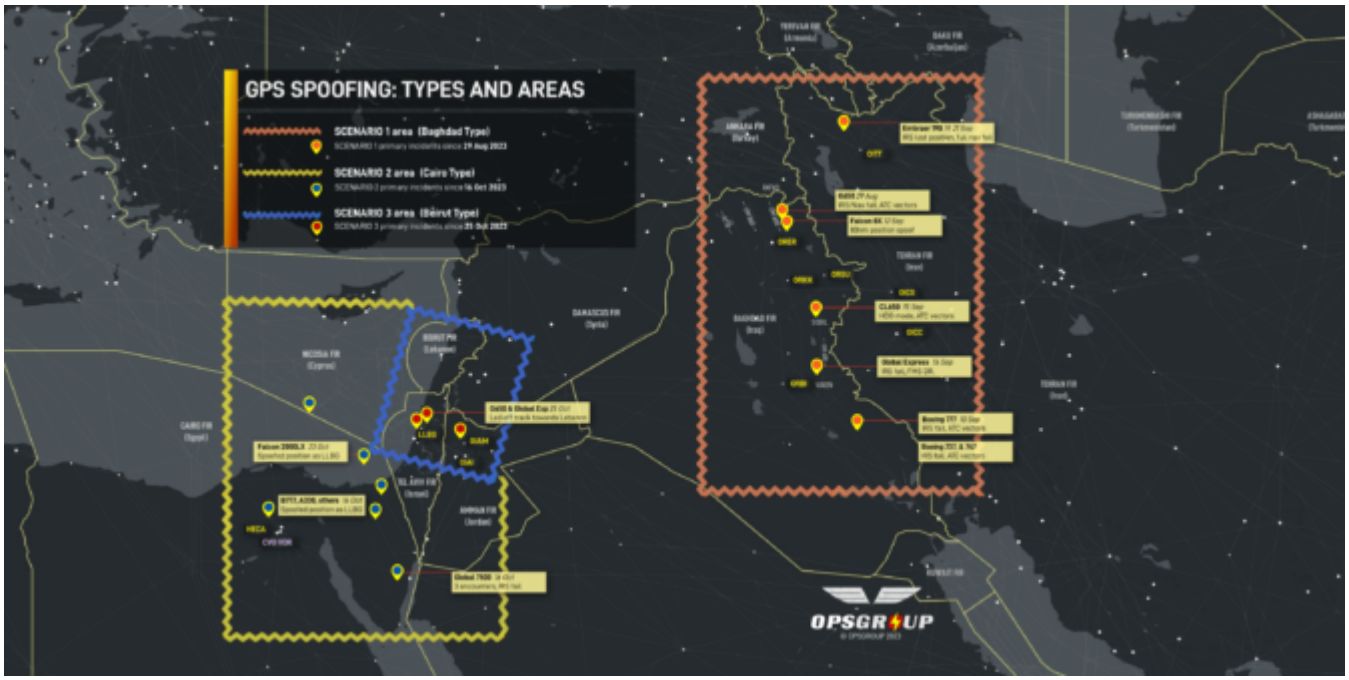
GPS Spoofing Update: Map, Scenarios and Guidance

Mark Zee
8 November, 2023



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.

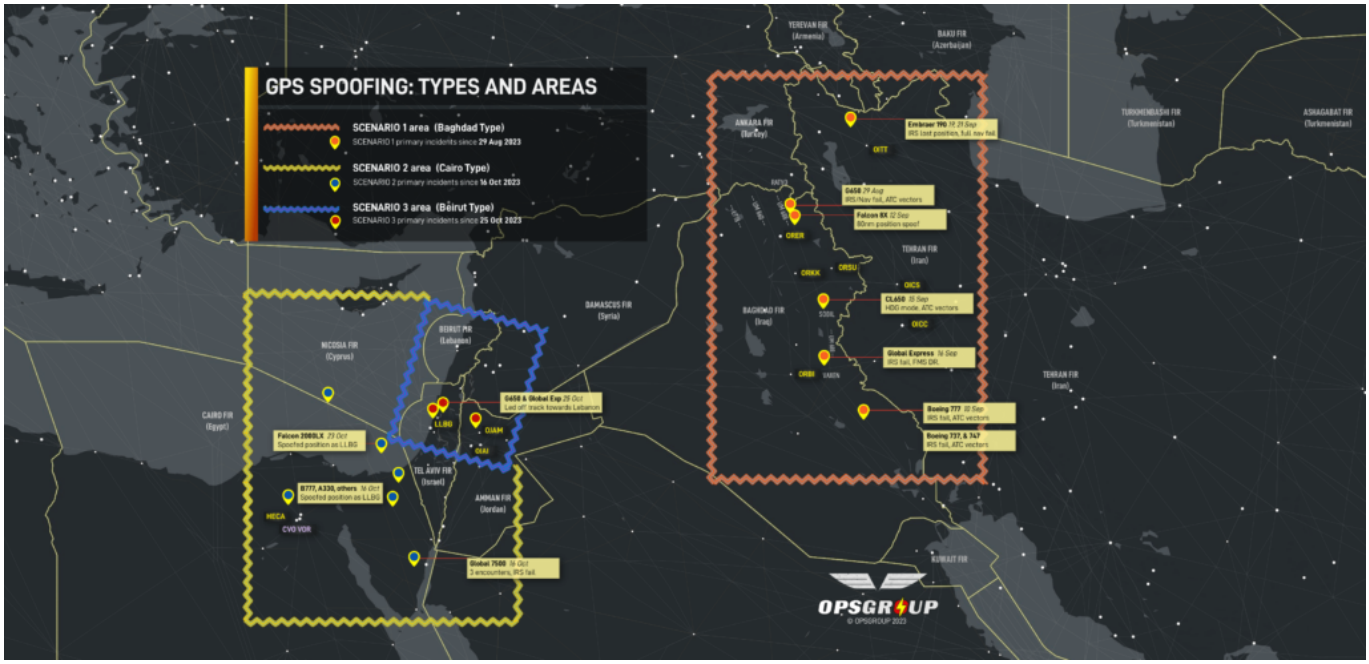
Two entirely new types of GPS spoofing have been reported in other areas since the first GPS Spoofing **report** we published on 26 September. These include **critical nav failures on departure from Tel Aviv leading aircraft towards Lebanon**, and spoofed signals received by multiple aircraft in the **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.



A high-res version is available here.

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

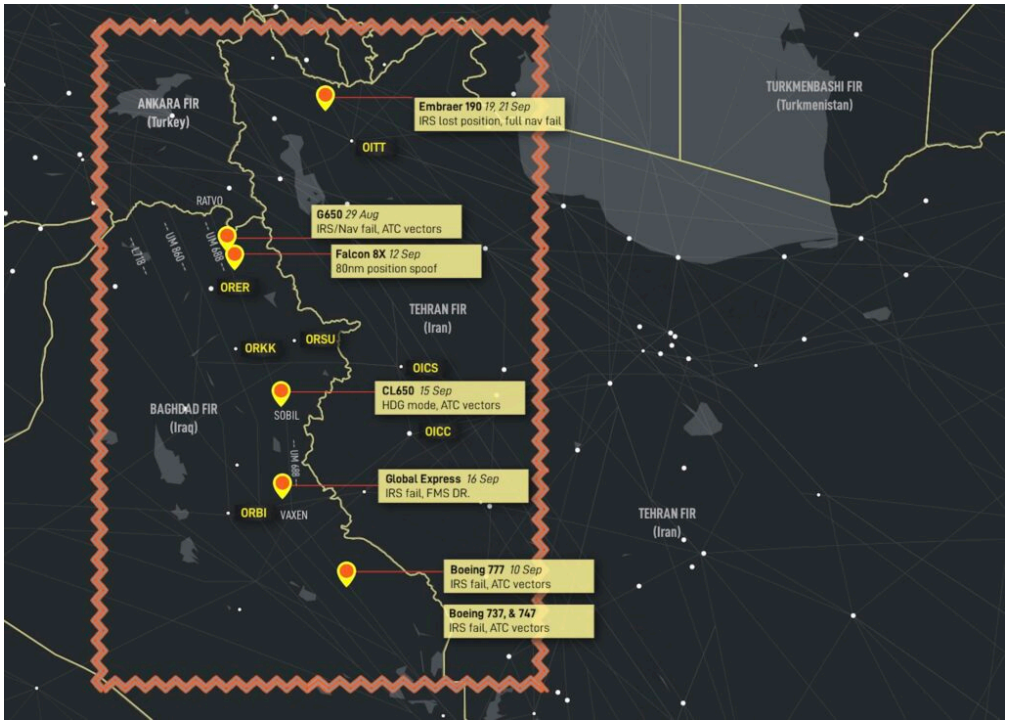
Worst case reports

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**

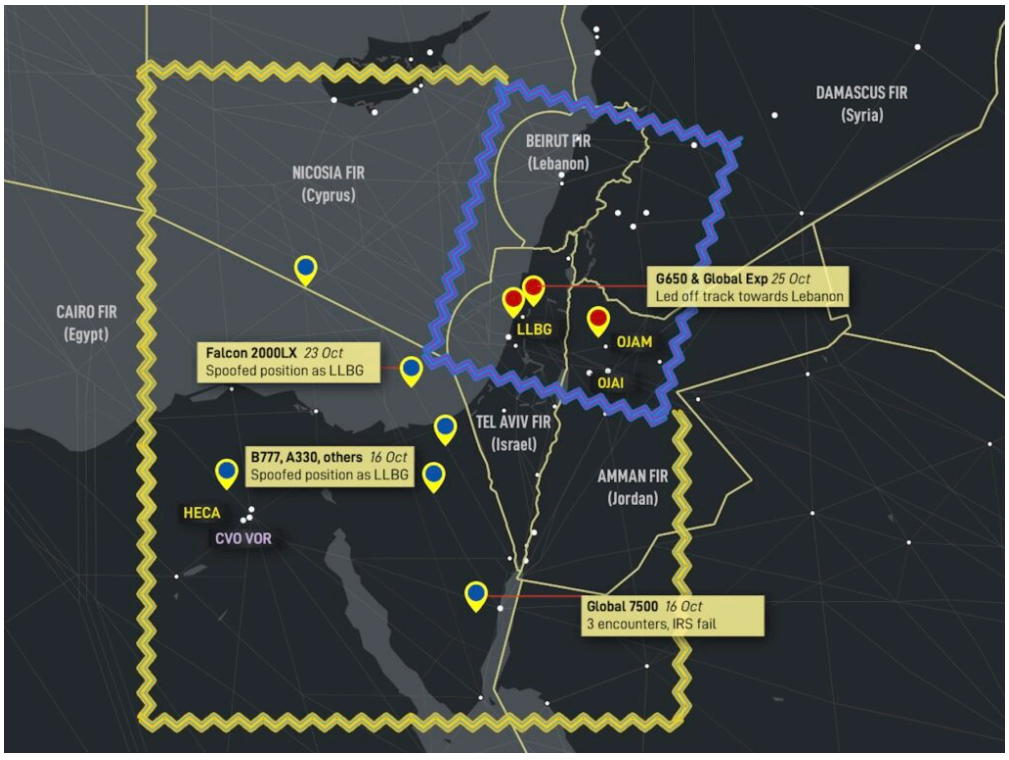


The **Baghdad** spoofing type involves GPS spoofing of enroute aircraft, nav failures follow. This was the first type of spoofing, initially reported on August 29, 2023, with a large amount of further reports starting in September 2023.

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)

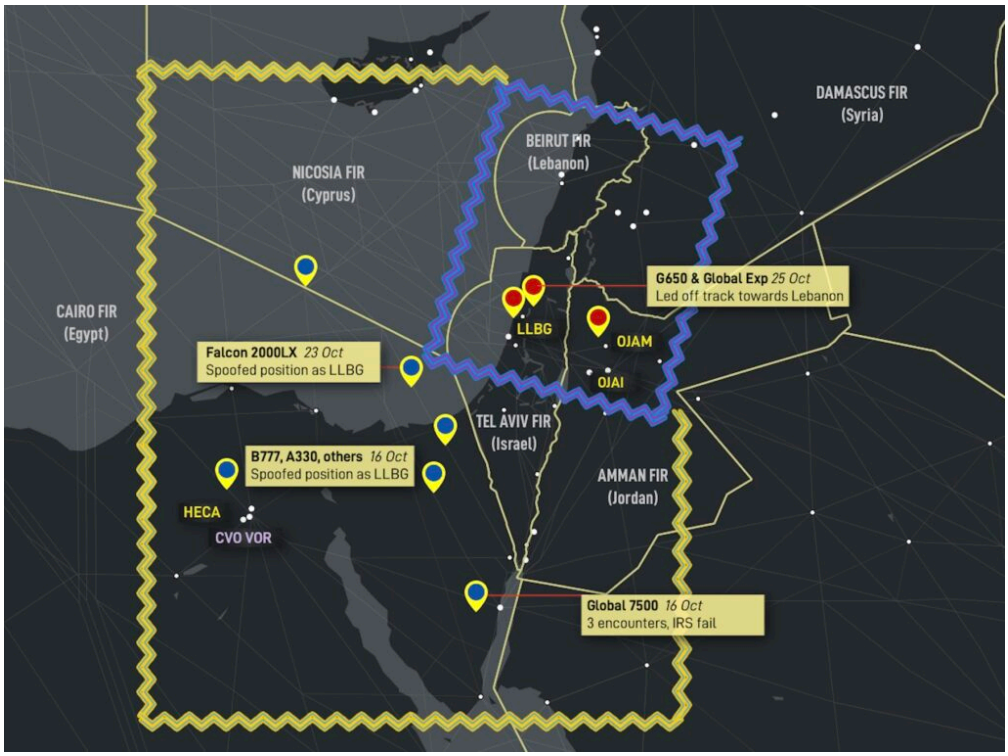


These reports first surfaced around Oct 16. Most reports are within the Cairo FIR. All crew reported similar circumstances, where a false or spoofed GPS position is received by the aircraft, incorrectly showing the aircraft position as being over LLBG/Tel Aviv. Locations vary from airways over the eastern 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)