FAA warning issued, further serious navigation failures reported

OPSGROUP Team
28 September, 2023



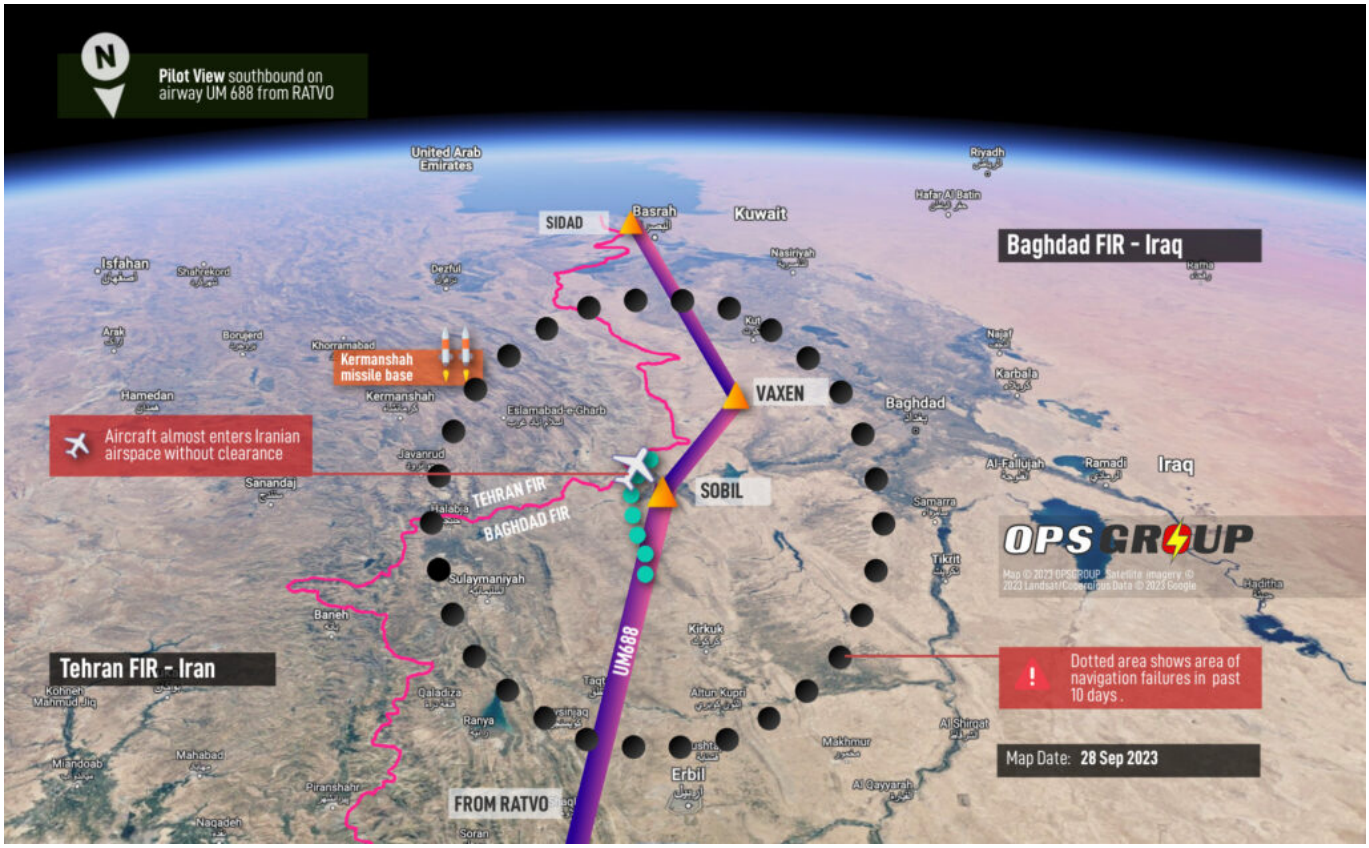
Since publishing Monday's **risk warning** on complex navigation failures following fake GPS signals, we have received further concerning reports from operators, mirroring the same events. The impact of the nav failures is becoming clearer, with one operator **almost entering Iranian airspace without 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.

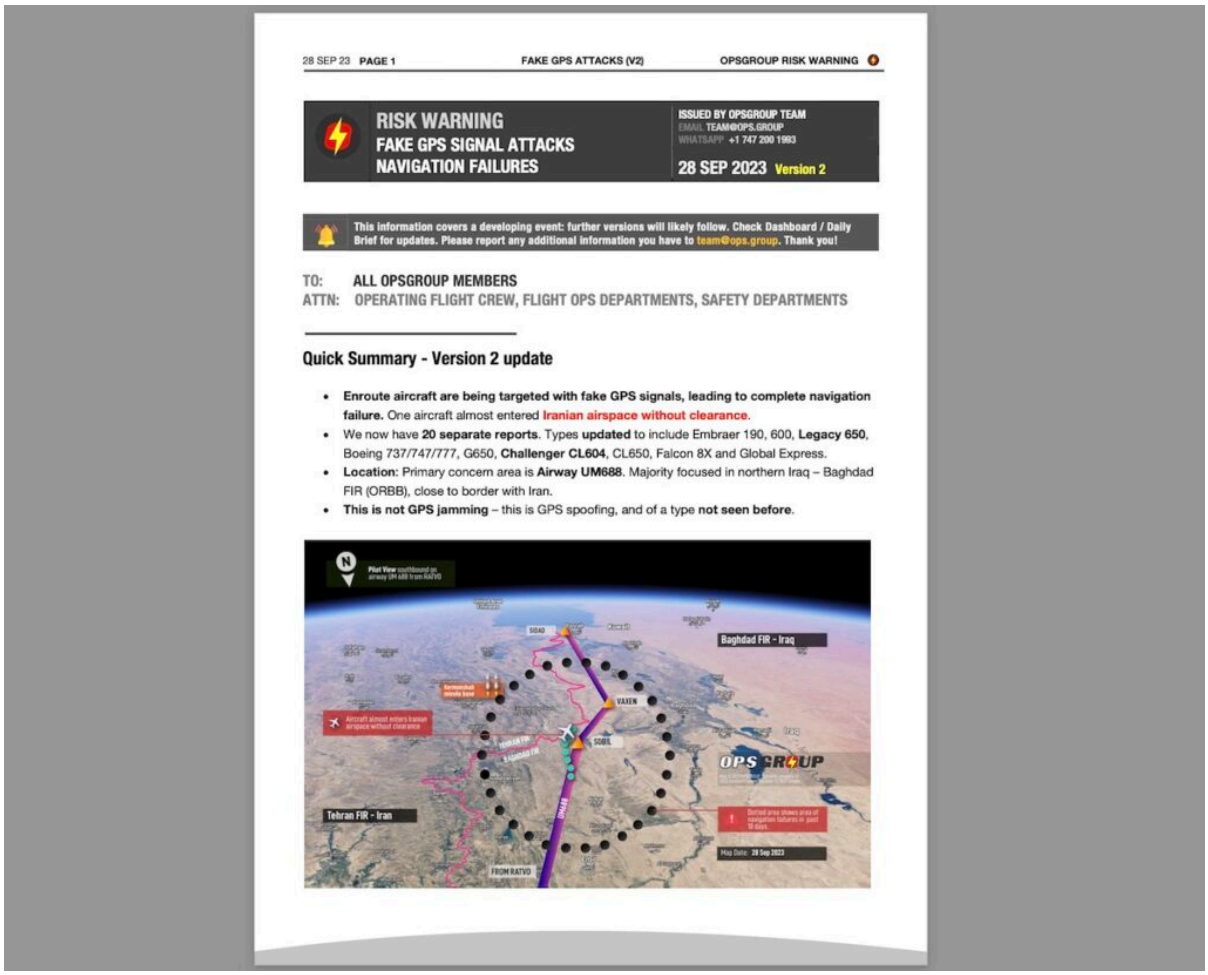
Exactly where the avionics problem arises as a result of these GPS spoofing signals is something that OEM's and Avionics providers are working on. However, **many modern IRS platforms include GPS updating while enroute, to correct drift**.

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

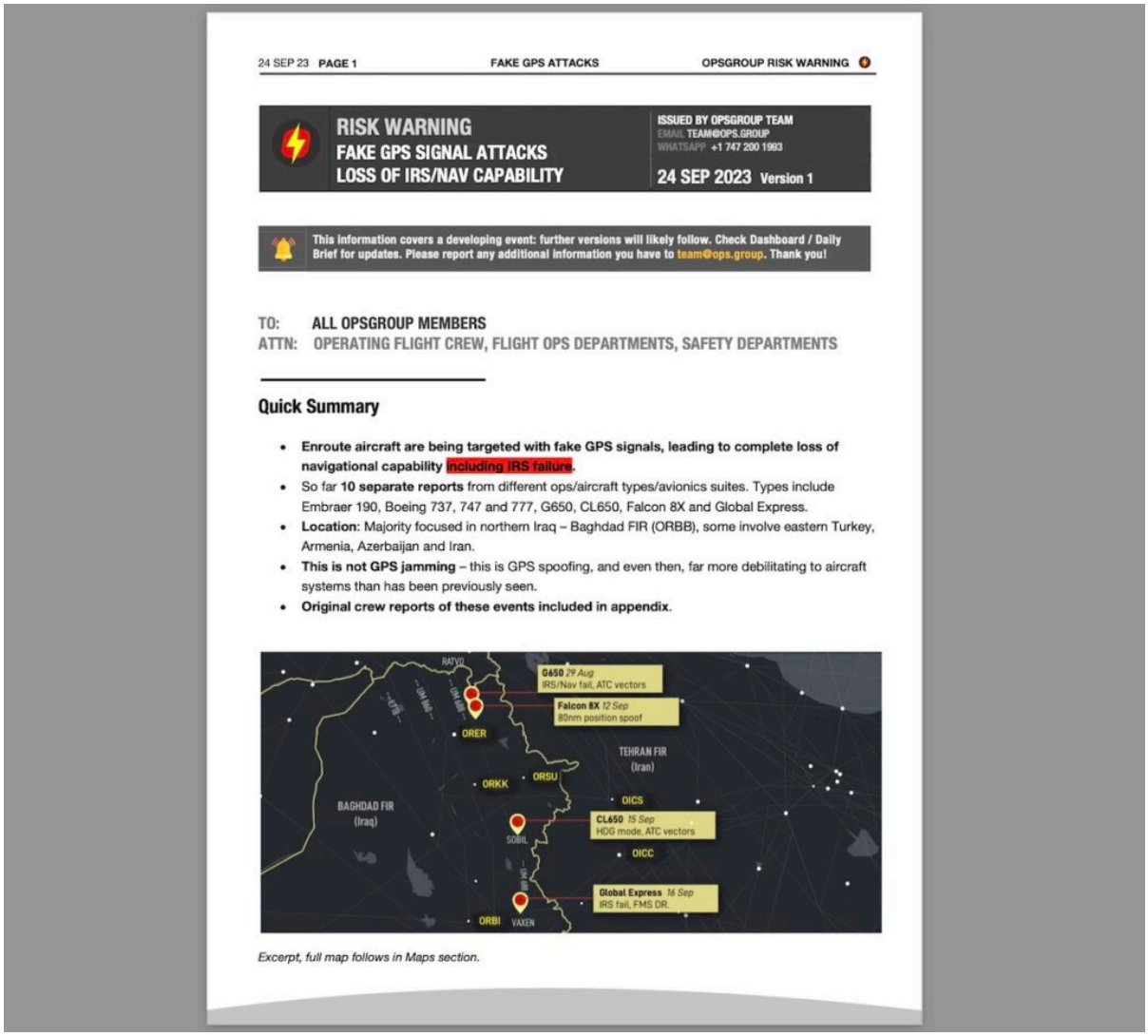
This information covers a developing event: further versions will likely follow. Check Dashboard / Daily Brief for updates. Please report any additional information you have to team@ops.group. Thank you!

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**