GPS Spoofing: Final Report published by WorkGroup

OPSGROUP Team
6 September, 2024

Key Points

- **Final Report of the GPS Spoofing Workgroup published today**
- **950 participants across full spectrum of aviation industry**
- **Significant concern regarding safety impact of GPS Spoofing**
- **Report download below**

Final Report Published

The Final Report of the GPS Spoofing WorkGroup has been published today, September 6th, 2024.

Over a six-week period between July 17-August 31, the WorkGroup tackled the complex issue of GPS Spoofing affecting civil aviation.

950 people participated in the project, representing the full spectrum of the aviation industry. Led by OPSGROUP, the WorkGroup comprised hundreds of commercial pilots, safety managers, and representatives from airlines, aircraft operators, and air traffic control. Additionally, a diverse group of aviation authorities, avionics manufacturers, aircraft manufacturers, and experts in GPS and GNSS systems participated. Industry organizations including EBAA, IFATSEA, IBAC, ALPA, IFALPA, the Dutch VNV, and BALPA contributed significantly. Support and expertise were also provided by various organizations and agencies, including the Royal Institute of Navigation, Eurocontrol, the Israel National Cyber Directorate, the UK Ministry of Defence, the UK Royal Air Force (RAF), NASA (Langley), U.S. Space Command, the German Aerospace Center (DLR), Zurich University of Applied Sciences, and the University of Texas.

The result is a comprehensive study of the GPS Spoofing problem, including detailed analysis of the technical background, impacts to aircraft handling and operation, best practices for flight crew, and a series of safety concerns and recommendations for industry attention.

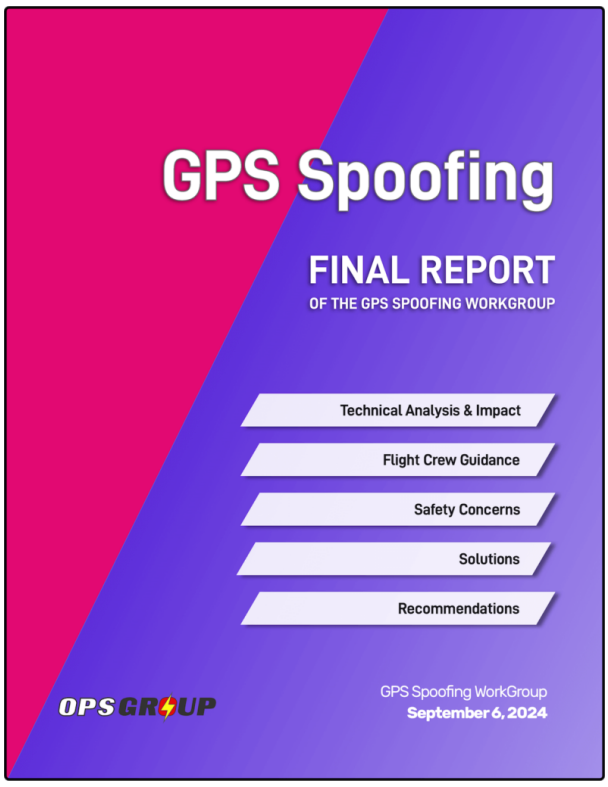
Overall, the Workgroup assessed that the impact of GPS Spoofing on flight safety, aircraft operation and handling, and ATC operations, is extremely significant. **The WorkGroup is very concerned about the overall impact of GPS Spoofing on flight safety**. A total of 8 overall safety concerns, and a further 33 specific concerns were raised.

This year, a 500% increase in spoofing has been observed. On average 1500 flights per day are now spoofed, versus 300 in Q1/Q2 of 2024. This is coincident with the summer months in spoofing affected areas. **With winter approaching**, the operating environment changes from predominantly good weather and VMC conditions, to poor weather, icing, and IMC conditions. **This change will increase the risk factors significantly.**

A survey of flight crew was carried out as part of the Workgroup. The response was excellent – almost 2,000 completed surveys were returned to the Workgroup. The results show that a full 1,400 crew members (~70%) rated their concern relating to GPS Spoofing impact on flight safety as very high or extreme. 91% of all crew members rated their concern as moderate or higher.

The future of GPS use in aviation is unclear. The Workgroup assessed that the vulnerabilities in public-use GPS that are now becoming evident (although known to experts for a decade or more), mean that the high involvement of GPS in aircraft systems is a major issue. Further, the over-reliance on GPS for primary navigation places great importance on preserving a sufficient network of conventional ground-based navaids. This aspect of the issue requires deeper study and conversation.

Download Final Report



Download the Final Report of the GPS Spoofing WorkGroup
PDF, 10 Mb, 128 pages.

Thank you!

Everything you see in this report is the result of community effort. If you know OPSGROUP, you know that this is our approach to solving problems in international flight operations. We have a strong, safety-focused industry, but sometimes things come up that affect us all, yet can't be solved by an individual aviation authority or group. GPS Spoofing is one such "thing".

This WorkGroup was truly something special. The participation of 950 individual people, across the entire industry – pilots, ATC, authorities, manufacturers, GPS experts, industry groups – is a marker of how much concern there is about the GPS Spoofing problem. But participation is just the first step. What stands out in this WorkGroup is the above-and-beyond efforts from so many participants.

Seemingly confounding technical questions were answered quickly, data was offered, contacts were sourced, ideas and solutions were hammered out into the small hours. For six weeks, we worked weekends and late nights, and no stone remained unturned. The energy, drive, and commitment of so many to solve this many-headed Hydra never faded.

There is so much knowledge, experience, and expertise in the international ops community, along with the key ingredient: a desire to share our skills, to tell each other what may harm us, to lead groups and to push for change. It's amazing to see.

Thank you to everyone who took part. From here, we hope that our efforts lead to better-informed flight crews, attention on the safety risks we have listed, and consideration of the recommendations presented at the end of this report.

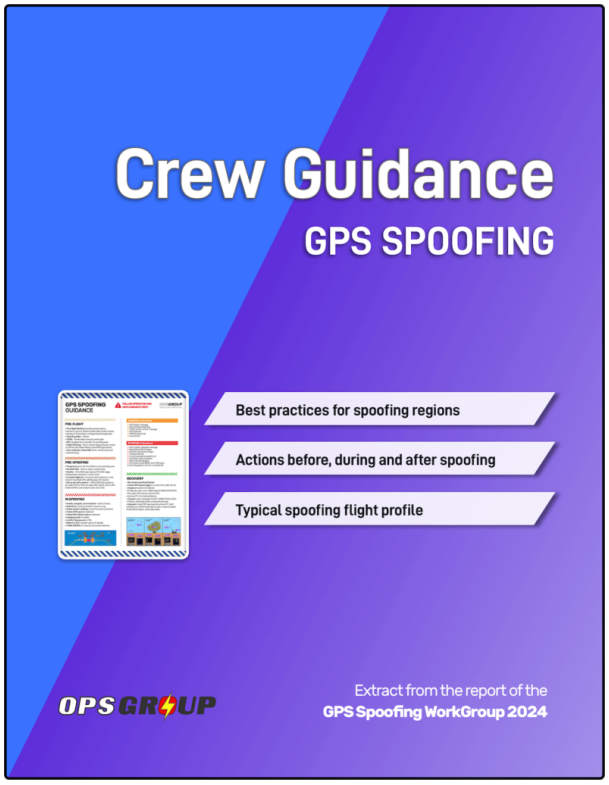
GPS Spoofing Guides

Some sections of the report were made available as reference guides, prior to the full release. These are available below.

Crew Guidance: GPS Spoofing

If you are operating a flight into a spoofing area tomorrow, this guidance will help to mitigate the impact of GPS Spoofing. This is based on best practices collected from the flight crew participating in the GPS Spoofing Workgroup, as well as OEM and other expert input.

- Best practices for spoofing regions
- Actions before, during and after spoofing
- Typical spoofing flight profile
- One-page Checklist style summary
- Diagrams: GPS Spoofing Flight Profile, GPS Reception during Jamming & Spoofing

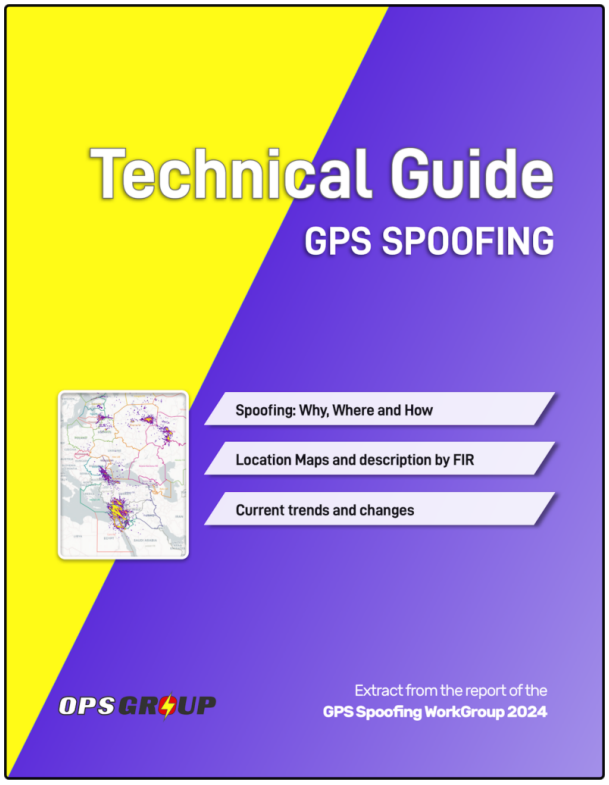


Download the Crew Guidance for GPS Spoofing, PDF, 2.7MB, 17 pages.

Technical Guide: the Where, Why and How of GPS Spoofing

This extract from the report of the GPS Spoofing Workgroup 2024 covers the technical details of GPS Spoofing:

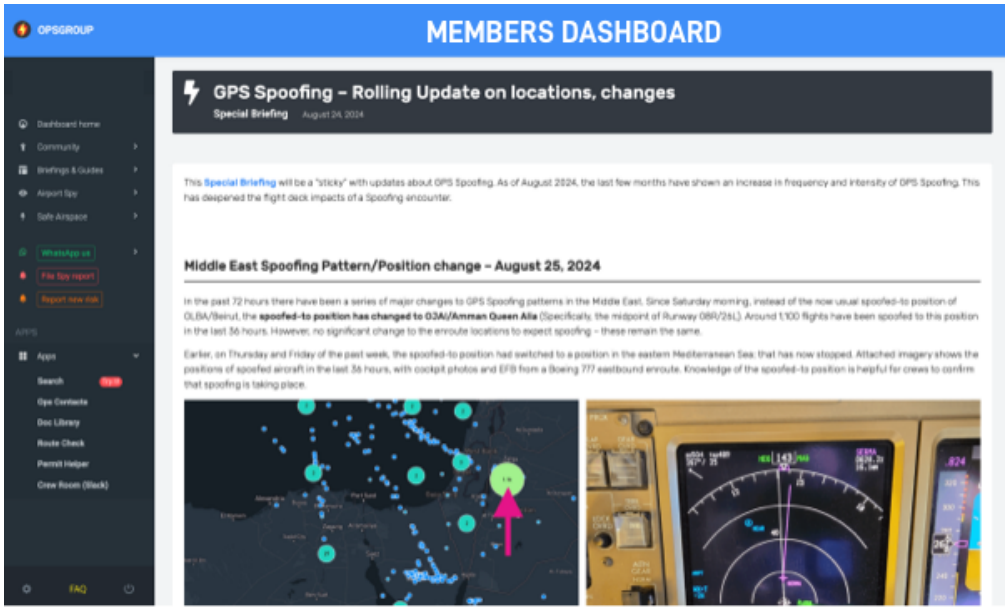
- Why, Where and How GPS Spoofing is happening – full technical details
- Location Maps: Worldwide, Mediterranean, Black Sea, Russia & Baltics, India/Pakistan
- Spoofing statistics and details by FIR
- Aircraft types affected
- Spoofing Patterns
- Changes and current trends



Download the Technical Guide to GPS Spoofing, PDF, 5.3MB, 29 pages.
[This links to the Guide, available in your Members Dashboard]

Ongoing GPS Spoofing Guidance

You can find a “rolling” **Special Briefing** in the Members Dashboard. This Special Briefing will be a “sticky” with updates about GPS Spoofing. As of August 2024, the last few months have shown an increase in frequency and intensity of GPS Spoofing. This has deepened the flight deck impacts of a Spoofing encounter.

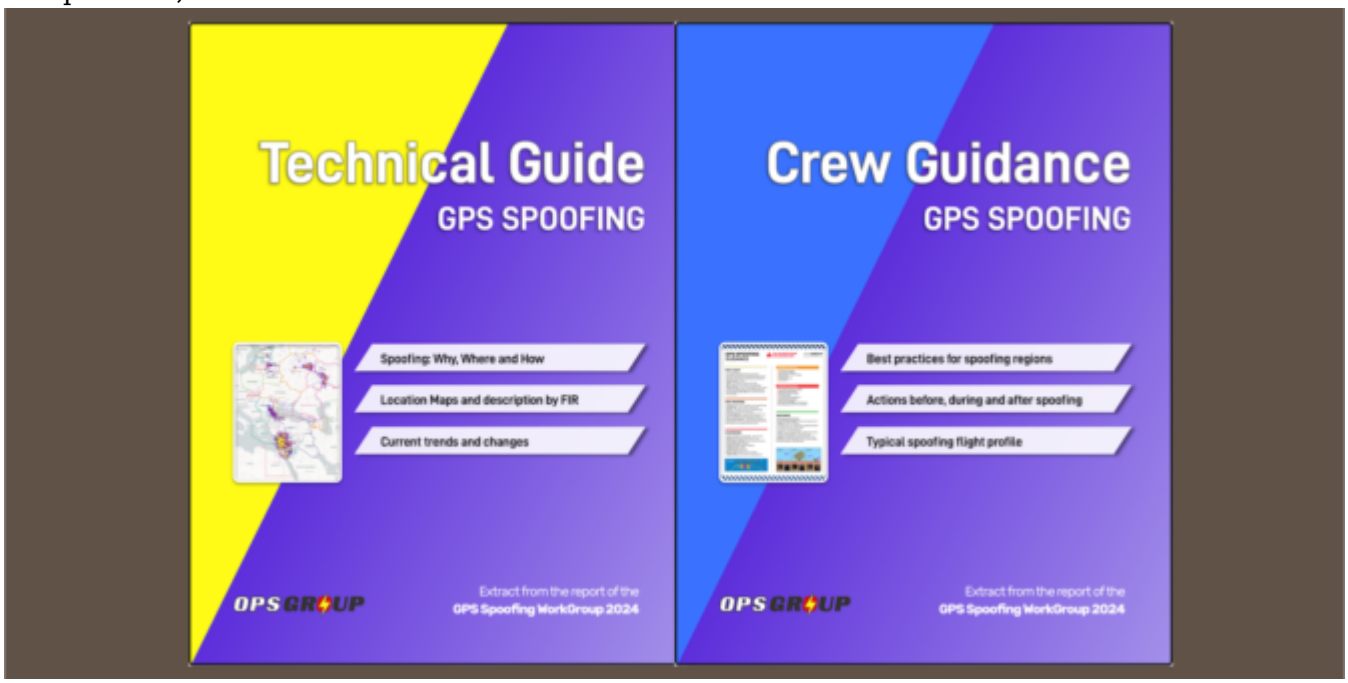


Special Briefing: GPS Spoofing – Recent updates:

- Middle East Spoofing Pattern/Position change – August 25, 2024
- Black Sea – Spoofing platform destroyed by Ukraine – August 15, 2024
- New Location: Western Ukraine – August 14, 2024
- New location: India/Pakistan border – July 2024
- 400% increase in GPS Spoofing – July 2024

Crew Guidance published by GPS Spoofing Workgroup

OPSGROUP Team
6 September, 2024



In August 2024, OPSGROUP co-ordinated a GPS Spoofing WorkGroup, to investigate **the GPS Spoofing problem**. The aim of the WorkGroup was to assess the impact, analyze safety risks, gather best practices and guidance for Flight Crew, and provide recommendations to industry. 950 people took part, from airlines and aircraft operators, ATC, aviation authorities, OEM's, GPS experts, and a variety of aviation organizations and other industry bodies.

Thank you to all who took part □□□. The Workgroup is now complete, and was a great success!

The complete report is available on this page. (after September 6th, 2024)

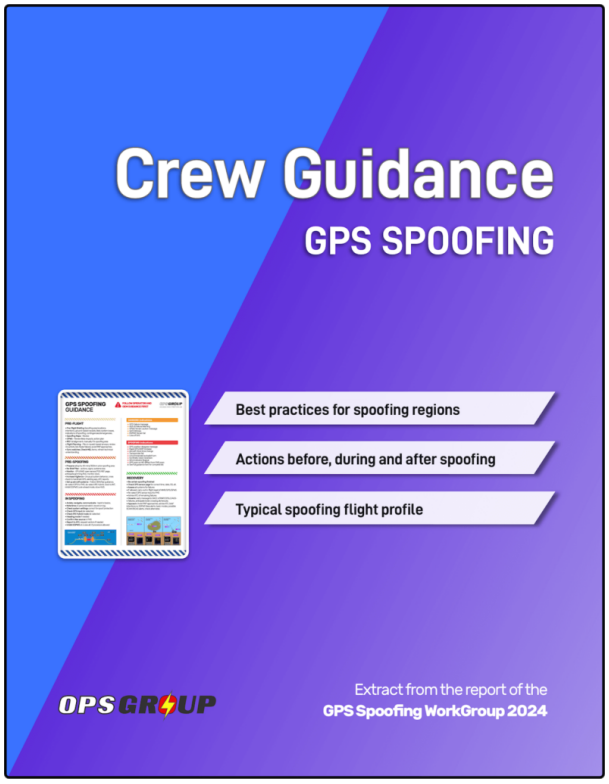
Report section extracts specifically for flight crew are below:

- **Crew Guidance**
- **Technical Guide: the Where, Why and How of GPS Spoofing**

Crew Guidance: GPS Spoofing

If you are operating a flight into a spoofing area tomorrow, this guidance will help to mitigate the impact of GPS Spoofing. This is based on best practices collected from the flight crew participating in the GPS Spoofing Workgroup, as well as OEM and other expert input.

- Best practices for spoofing regions
- Actions before, during and after spoofing
- Typical spoofing flight profile
- One-page Checklist style summary
- Diagrams: GPS Spoofing Flight Profile, GPS Reception during Jamming & Spoofing



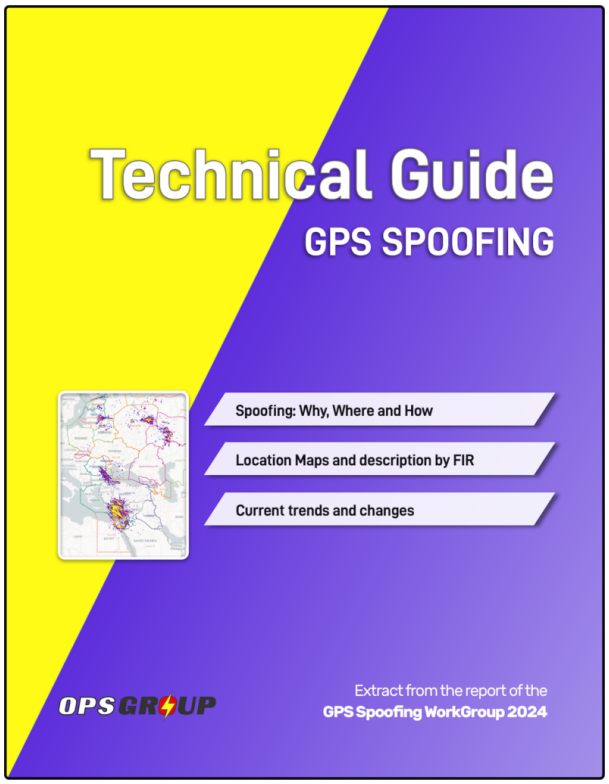
Download the Crew Guidance for GPS Spoofing, PDF, 2.7MB, 17 pages.

Technical Guide: the Where, Why and How of GPS Spoofing

This extract from the report of the GPS Spoofing Workgroup 2024 covers the technical details of GPS

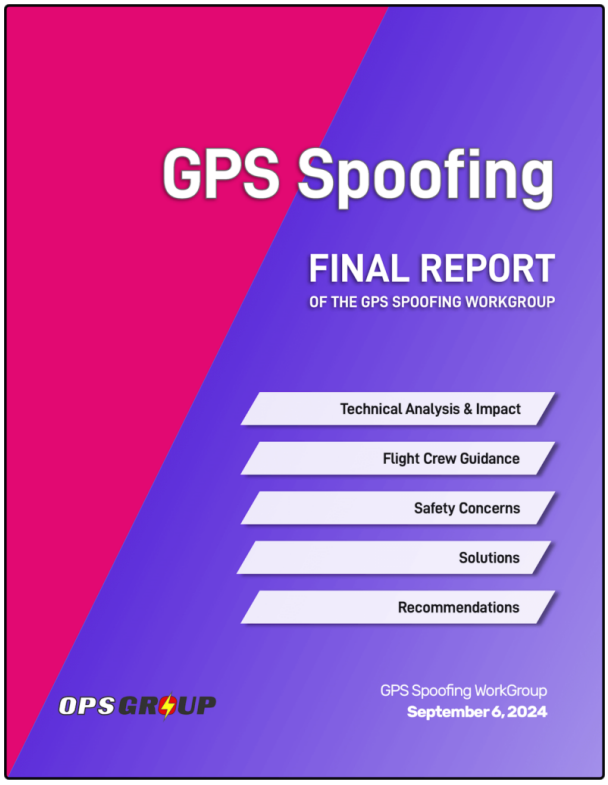
Spoofing:

- Why, Where and How GPS Spoofing is happening – full technical details
- Location Maps: Worldwide, Mediterranean, Black Sea, Russia & Baltics, India/Pakistan
- Spoofing statistics and details by FIR
- Aircraft types affected
- Spoofing Patterns
- Changes and current trends



Download the Technical Guide to GPS Spoofing, PDF, 5.3MB, 29 pages.
[This links to the Guide, available in your Members Dashboard]

Final Report



Link to the Final Report of the GPS Spoofing WorkGroup.
PDF, 10 Mb, 128 pages.

400% increase in GPS Spoofing; Workgroup established

OPSGROUP Team
6 September, 2024

GPS Spoofing Risk changes, grows

- **900 flights a day on average are now encountering GPS Spoofing**
- **Safety risks changing and growing: EGPWS primary concern**
- **GPS Workgroup established to address issue**

Troubling data shows a significant spike in GPS Spoofing over the last few months, with an increasing impact on flight safety.

The number of flights affected has risen from an average of 200 daily in the period January-March, to around 900 daily for the second quarter of 2024. On some days, as many as 1350 flights have encountered spoofing. Flight crews also report that the intensity of the spoofing is increasing.

At the same time, the number of locations where spoofing is highly active has increased from three to more than ten. At the outbreak of the new spoofing phenomenon in September 2023, spoofing was encountered in northern Iraq (near Baghdad), Egypt (near Cairo), and Israel. Since then, the Black Sea, Cyprus, the Korean border, and Russia have become spoofing hotspots.

Safety risk changing and growing

For flight crews, the workload and knock-on safety risk resulting from spoofing encounters is both changing and growing. Initially, the primary risk from a GPS spoof was navigational: autopilots began turning aircraft unexpectedly, aircraft position became uncertain, IRS was sometimes lost. With ATC help, often through radar vectors, the situation could be resolved.

With both the increase in intensity and frequency of spoofing this year, a second, more concerning set of risks is emerging.

The list is long. GPS is interwoven into many, if not most, aircraft systems these days. The EGPWS – our trusted friend to keep us away from terrain – is suffering heavily, and is becoming unreliable. False alerts – sometimes hours after the spoofing event – are now routine, and as a result, many are inhibiting the system. Crews are losing trust in what was until now an exceptionally reliable and critical device to eliminate CFIT accidents.

Go-arounds directly caused by GPS spoofing effects are also being seen more regularly. False EGPWS alerts are the primary culprit, but in some cases, the indicated wind on the Navigation Display is false and leads to confusion. In others, autopilot behaviour and unusual glideslope/localizer indications are causing missed approaches. Any go-around immediately increases crew workload and reduces the safety margin.

Safety layer of “Swiss Cheese” removed

Other aircraft systems directly affected include TCAS, ADS-B, HUD guidance, and transponders. The aircraft clock, which crews are getting used to seeing “run backwards”, is often one of the first victims of a spoofing encounter, and has knock-on effects which include making CPDLC unusable. Eurocontrol report now seeing this on a daily basis.

For Air Traffic Control, especially in Oceanic and remote regions requiring on-board responsibility for

navigation accuracy, life has thus become more challenging. Shanwick and Gander OACC's now deal daily with aircraft unable to meet the RNP4 requirement for oceanic crossings as a result of spoofing. Controllers have to work harder to separate aircraft, and this has caused occasional diversions to Iceland.

The trouble is that these shifts in safety risk are happening without much attention to them. They are largely unaddressed, latent pitfalls, that will become painfully clear when the first accident attributable to spoofing occurs. A single, full layer of the "Swiss Cheese" has quietly been pulled out of our safety system this year.

GPS Spoofing Workgroup established

A GPS Spoofing Workgroup has been hastily established to bring the international civil aviation community together and address the problem. The Workgroup is **now running,** and will tackle the issue by collecting data and information, surveying flight crew, discussing the distinct elements of the problem, and producing a community report. With the 14th ICAO Air Navigation Conference taking place at the end of August, the timing of the final report will aim to support discussions there.

450 participants have registered to take part in the Workgroup, which includes representatives of industry organizations IFALPA, IFATCA, OPSGROUP, IBAC, EBAA, ECA, and BALPA. Airlines and Operators represented include Aer Lingus, Air Atlanta, Alaska Airlines, Cathay, Cargolux, Singapore Airlines, Turkish Airlines, United Airlines, Netjets, El Al, Royal Jordanian, Italian Air Force, USAF, American Airlines, LOT Polish Airlines, and Fedex.

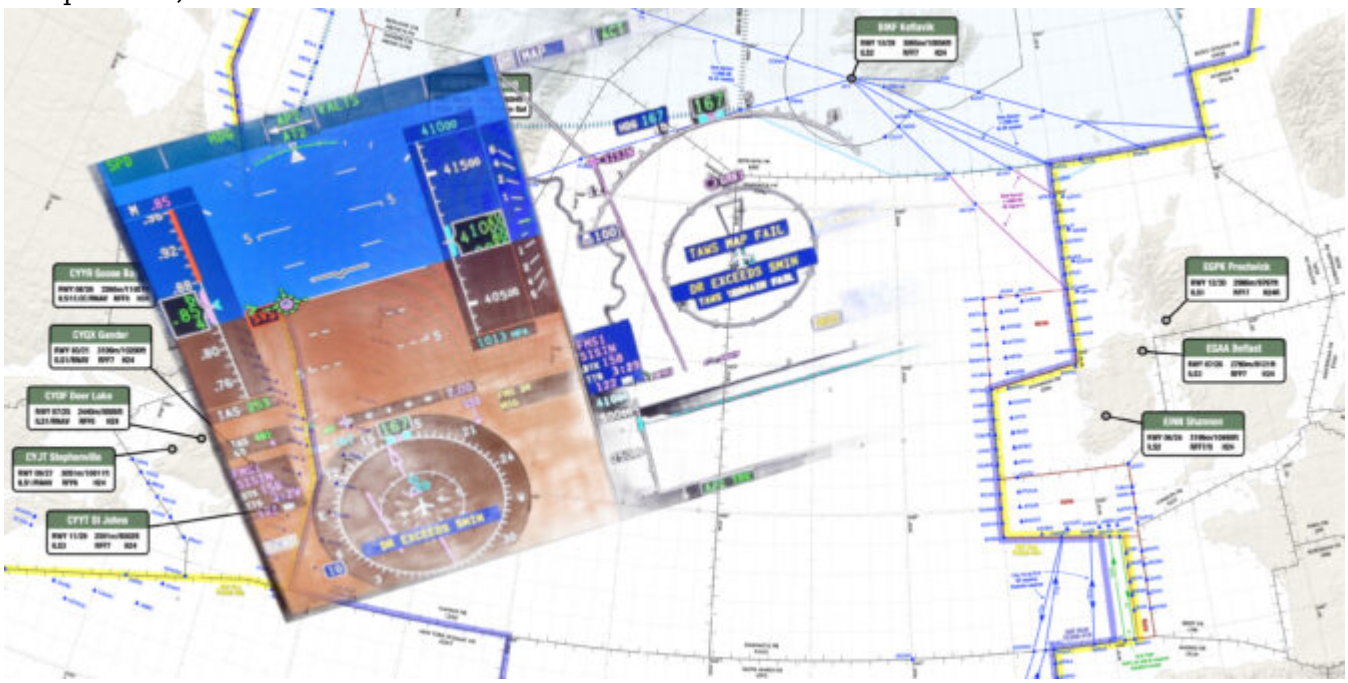
An encouraging element of the Workgroup is the involvement of PNT and GPS experts from NASA, Boeing, Collins Aerospace, FlightSafety International, Honeywell International, Safran Electronics & Defense, Satcom Direct, Aircraft Performance Group, Fokker Services, Honda Aircraft Company, Zurich University of Applied Sciences, and SkAI Data Services. Aviation Authorities participating include the Swedish CAA, Transport Canada Civil Aviation, Civil Aviation Authority of Singapore, Civil Aviation Authority of Thailand, CAA Isle of Man, Eurocontrol, FAA, and NATS UK.

To date, the industry has largely focused on ad-hoc mitigation efforts to deal with the GPS Spoofing problem. The focus of the Workgroup will be to shift to discussing quickly available solutions, and broaden industry awareness of the growing safety risks. It will also seek to provide Flight Crews with better guidance, actions and GPS systems information.

The Workgroup is now complete. A final report will be published on September 6, 2024.

NAT Crossing after GPS spoofing: a guide

Mark Zee
6 September, 2024



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**.

Outsmarting the GPS spoofers: A clever app

Andy Spencer
6 September, 2024

GPS spoofing is fast becoming a real headache in aviation, causing **confusion and navigation problems for pilots** in several hotspots around the world.

We first saw this happening in September 2023, when we started getting reports of spoofing across the Middle East, including instances near **Iraq, Iran, Egypt, Israel, Jordan, Turkey, Cyprus, and Lebanon.**

Since then we've had reports from all kinds of strange places including **Pakistan, Niger, and China.**

GPS spoofing involves **sending false GPS signals to aircraft**, leading to potential navigation errors and safety risks.

Manufacturers have been slow to work out **what advice to pass on to pilots and operators** on how to counteract these issues. But the effectiveness of these measures can be limited without the right tools, especially during live spoofing events where the reliance on ATC becomes critical.

NaviGuard, developed by APG, is a **new tool designed to counter GPS spoofing threats**. It's a plotting application that uses traditional ground navigation aids (e.g., VORs, DMEs, NDBs) to cross-check and verify the aircraft's GPS-reported position. And best of all – **it's free.** You can download it here.

When NaviGuard **detects discrepancies indicative of GPS spoofing**, it alerts the pilots with a clear "GPS anomaly detected" message, enabling them to take corrective action promptly.

NaviGuard offers pilots a straightforward solution for maintaining navigational accuracy amidst GPS spoofing threats.

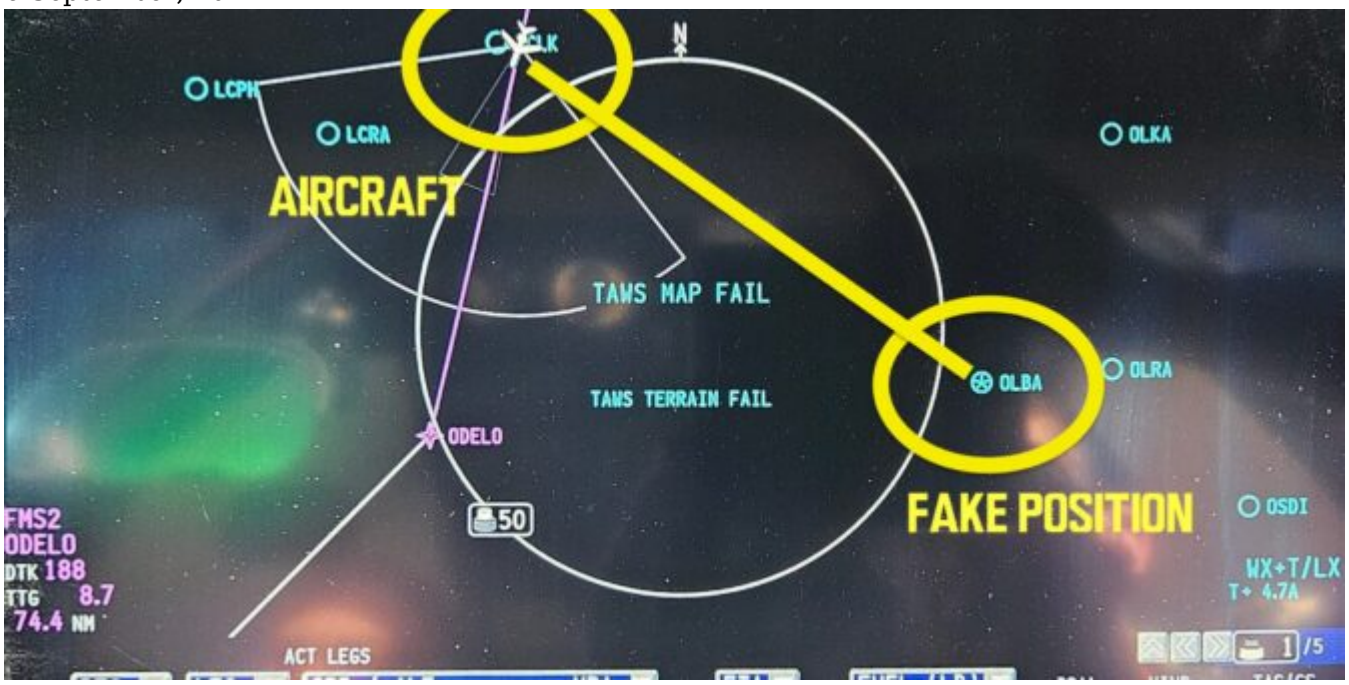
I used NaviGuard last month when I was spoofed whilst operating in Cairo. I got to try out the app for 30 minutes **while our GPS tried to convince us that we were flying on top of Beirut.**

As promised by Michael and the team at APG, the app was easy to use, and it allowed me to **quickly verify that my IRS position was not compromised** (we have a Hybrid IRS, so a spoofed GPS signal can corrupt the position data).

This is a no-bells-or-whistles solution, which I believe is an excellent addition to any pilot's EFB; after this flight, I installed the app on all of our aircraft's EFBs. It takes up very little space and is free. **This is the great insurance when doubting your GPS position's integrity.**

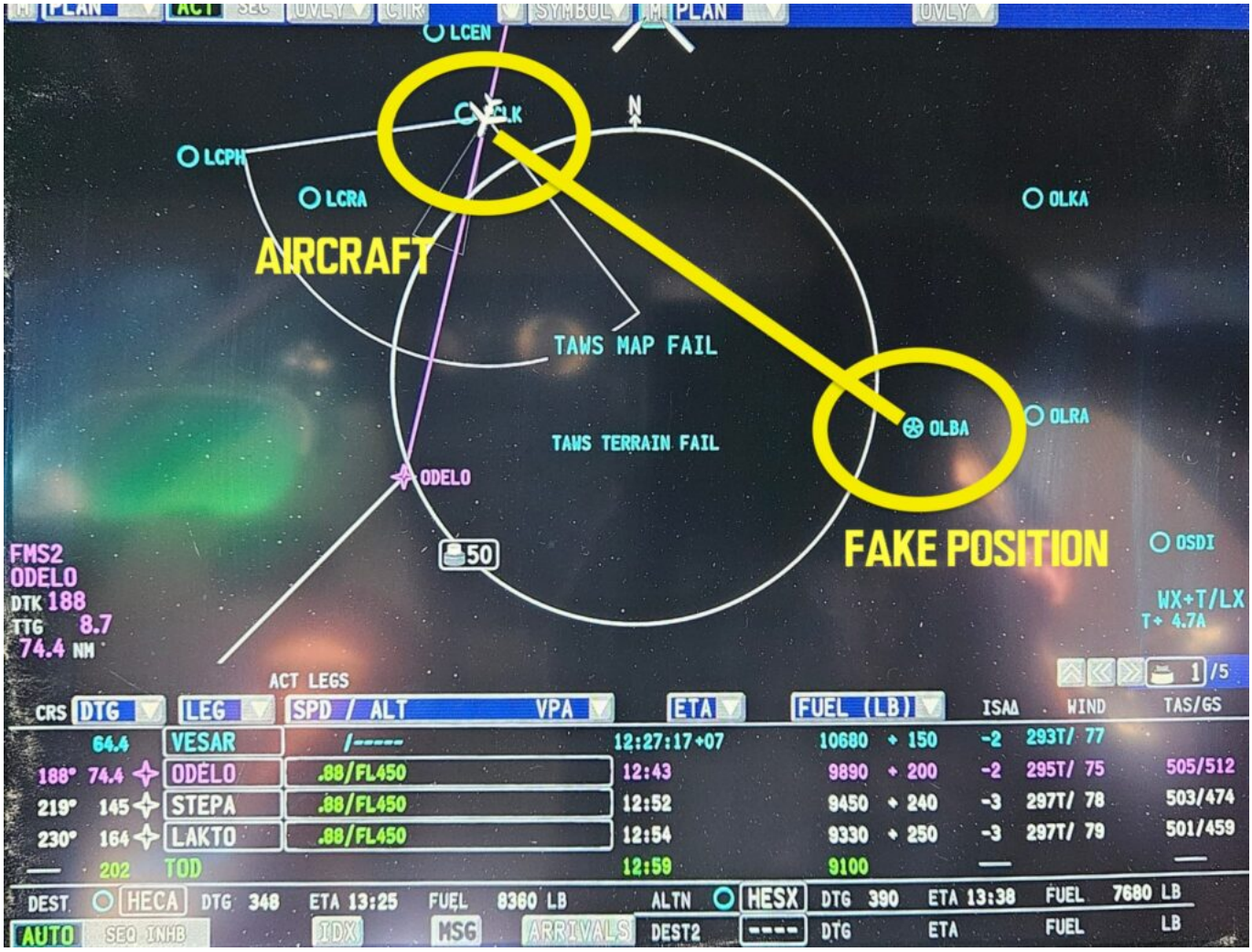
New GPS spoofing incident shows how it works

OPSGROUP Team
6 September, 2024



An OPSGROUP member reported a new **GPS spoofing encounter** yesterday in the Ankara FIR, while flying southbound between UDVET and INPOR.

The encounter began around 1200Z, when both selected GPS positions **began to show the aircraft position as being over OLBA**/Beirut – approx **120nm away**.



The crew had disabled GPS inputs prior to the area, but briefly selected them again on the PNF side – when the spoofing began. The route flown during the event was essentially a straight line from LTAF/Adana to LCLK/Larnaca.

The aircraft was a Global Express 7500 at FL470. OLBA/Beirut is in one of the three hotspot areas for GPS spoofing, but this one over Adana is perhaps the furthest away yet to report the problem.

Analysis

This is a great example of how GPS spoofing works. The Nav Display shows the fake **GPS position** with the star symbol – located exactly at OLBA/Beirut airport.

The **aircraft position** however – thanks to the crew disabling GPS sensors – is correctly shown over LCLK/Larnaca.

If the crew had not proactively disabled those sensors, the aircraft position would also be shown as over OLBA – and if the spoofing was subtle, the FMS would tend to start suggesting a right turn back to the track inbound ODELO.

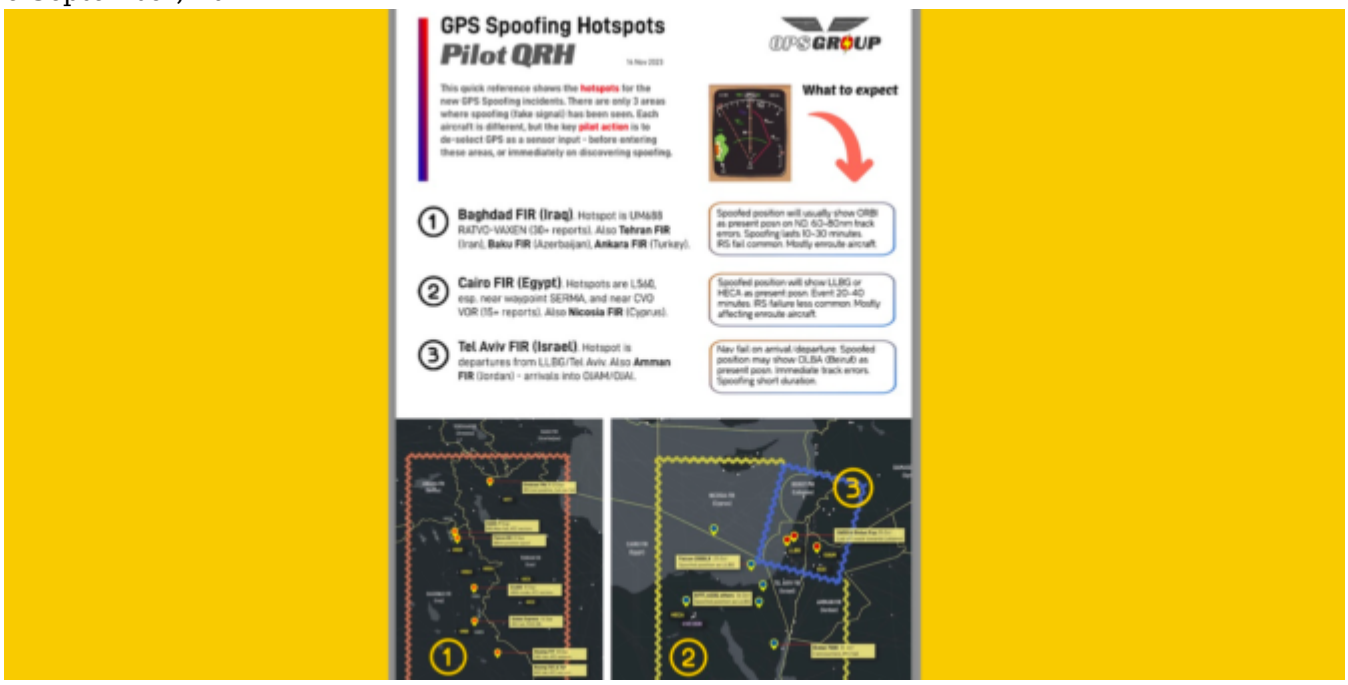
Further reading:

- GPS Spoofing Hotspots

- GPS Spoofing QRH – Pilot Guide
- Nov 8 update – Maps, Scenarios, Guidance
- Special Briefings on GPS Spoofing (with reports)

GPS Spoofing: Pilot QRH – Hotspots and What To Expect

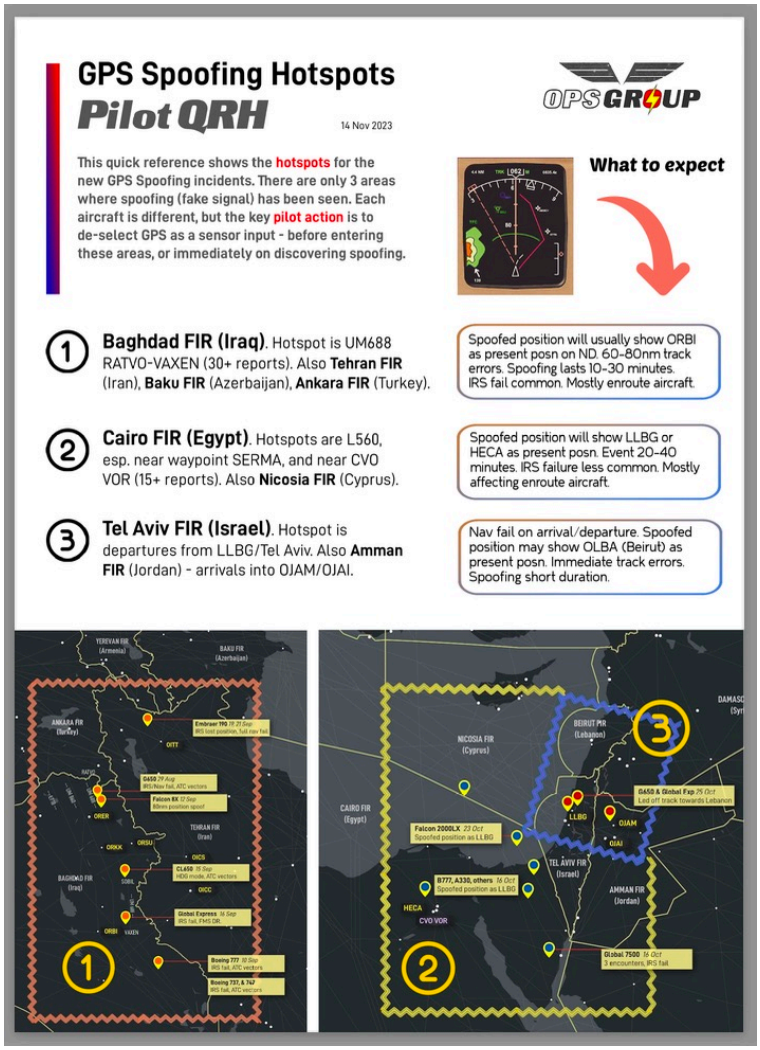
OPSGROUP Team
6 September, 2024



This quick reference shows the hotspots for the new GPS Spoofing incidents.

There are only 3 areas where spoofing (fake signal) has been seen. Each aircraft is different, but the key pilot action is to de-select GPS as a sensor input – before entering these areas, or immediately on discovering spoofing.

Download the OPSGROUP GPS Spoofing Hotspots – Pilot QRH (14 Nov 2023)

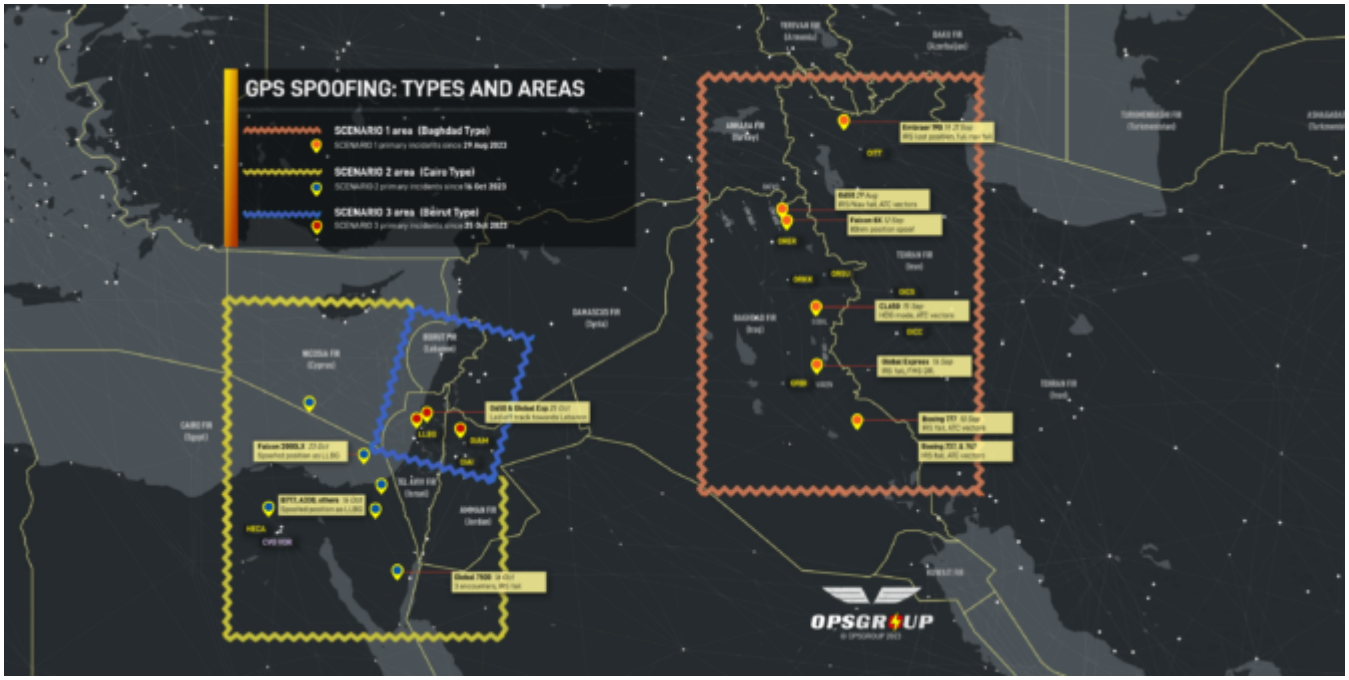


For further on this topic:

- GPS Spoofing update (Nov 8, 2023)
- GPS Spoofing: FAA warning (Sep 28, 2023)
- GPS Spoofing: First reports (Sep 26, 2023)

GPS Spoofing Update: Map, Scenarios and Guidance

Mark Zee
6 September, 2024



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

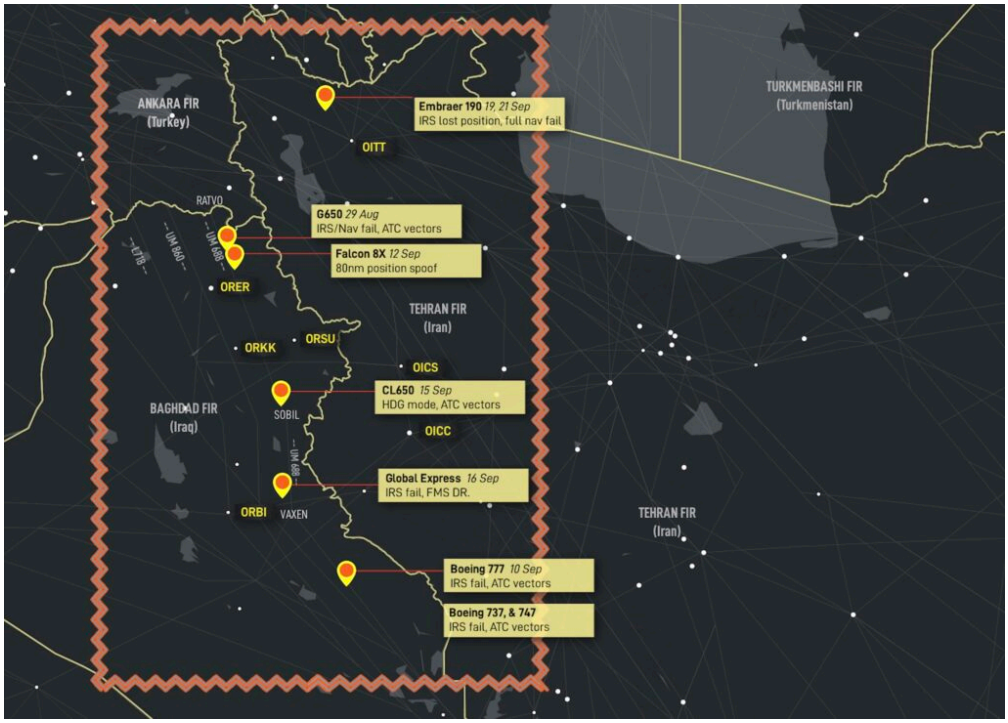
In all, OPSGROUP has received close to 50 reports of GPS spoofing activity. Further down, we identify **three distinct spoofing scenarios** reported by flight crew. First, we highlight the most troubling reports to show how critical the impact can be.

- 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**

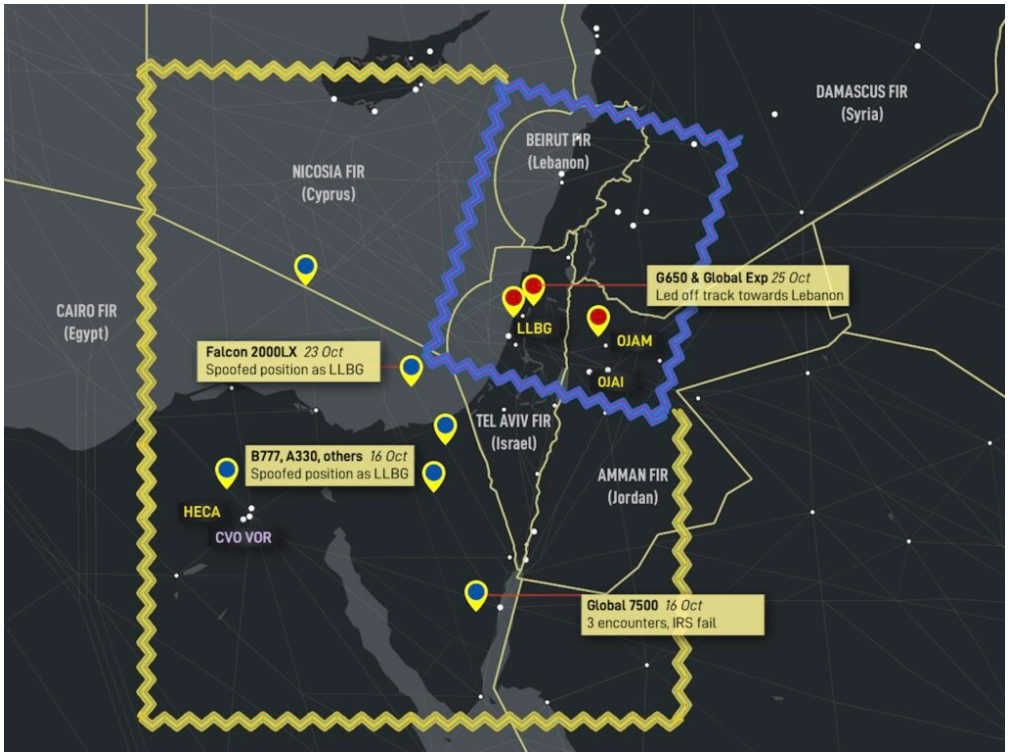


The **Baghdad** spoofing type involves GPS spoofing of enroute aircraft, nav failures follow. This was the first type of spoofing, initially reported on August 29, 2023, with a large amount of further reports starting in September 2023.

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)

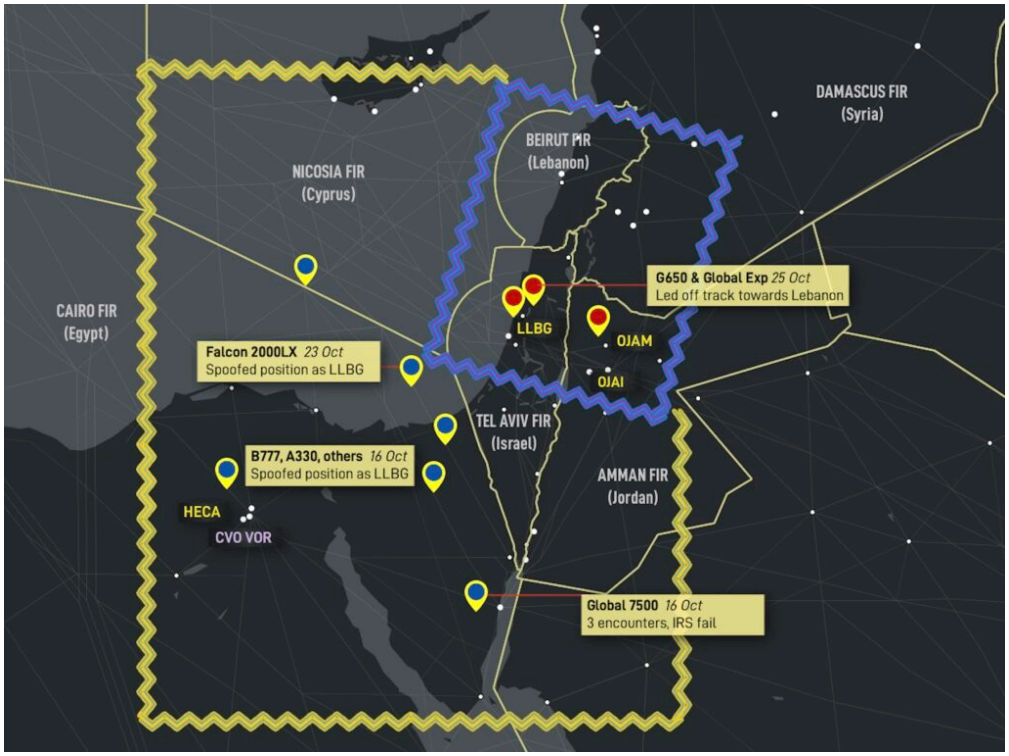


These reports first surfaced around Oct 16. Most reports are within the Cairo FIR. All crew reported similar circumstances, where a false or spoofed GPS position is received by the aircraft, incorrectly showing the aircraft position as being over LLBG/Tel Aviv. Locations vary from airways over the eastern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