400% increase in GPS Spoofing; Workgroup established

OPSGROUP Team
17 July, 2024

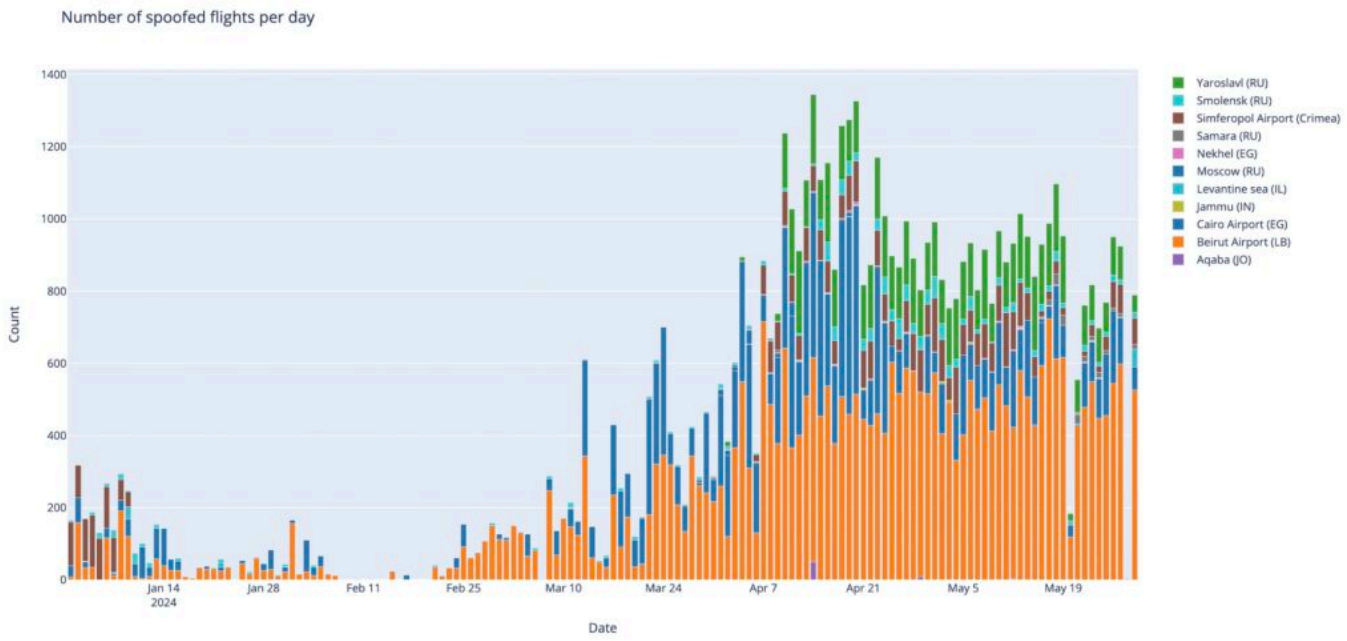


GPS Spoofing Risk changes, grows

- **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.



Graph shows number of flights affected by spoofing, broken down by location. Data from Zurich University of Applied Sciences & SkAI Data Services.

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.

INDUSTRY COLLABORATION

GROUP DISCUSSION
INFO GATHERING
IMPACT REVIEW

FLIGHT CREW // TECH EXPERTS // OEM'S
OPERATORS // INDUSTRY GROUPS // ATC
A/C MANUFACTURERS // REGULATORS



WORKGROUP REPORT

CREW GUIDANCE
SAFETY REVIEW
SITUATION REPORT
LOCATION MAP
SECURITY ANALYSIS
RECOMMENDATIONS

GPS SPOOFING WORKGROUP

JULY 17 – AUG 14 REGISTER NOW