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.

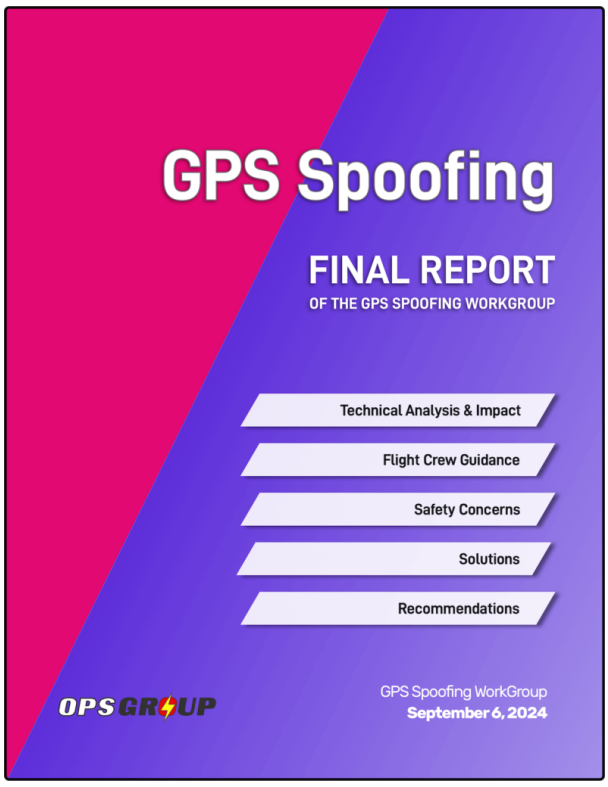
Overall, the Workgroup assessed that the impact of GPS Spoofing on flight safety, aircraft operation and handling, and ATC operations, is extremely significant. **The WorkGroup is very concerned about the overall impact of GPS Spoofing on flight safety**. A total of 8 overall safety concerns, and a further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

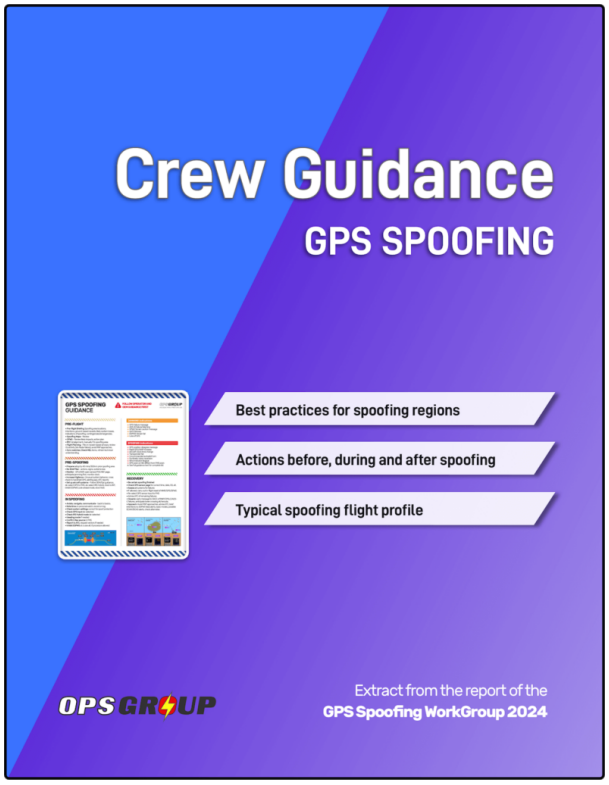
GPS Spoofing Guides

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

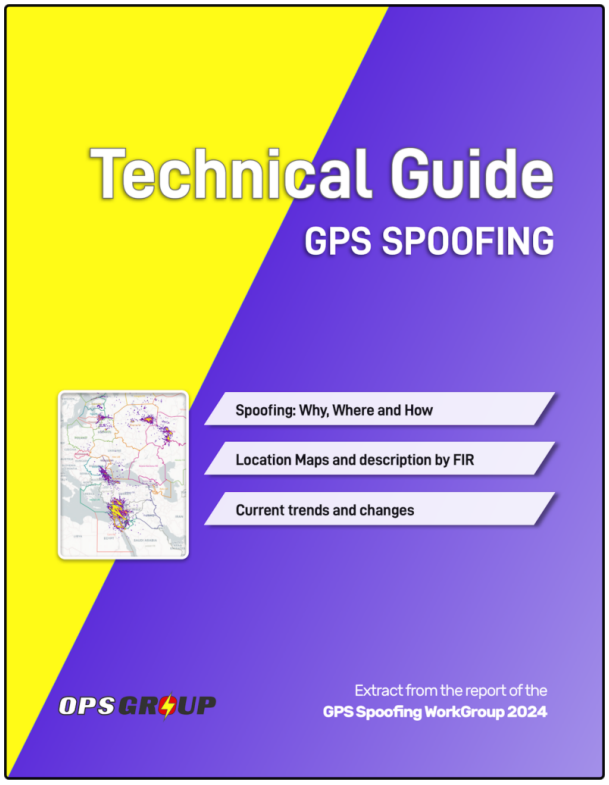


Download the Crew Guidance for GPS Spoofing, PDF, 2.7MB, 17 pages.

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:

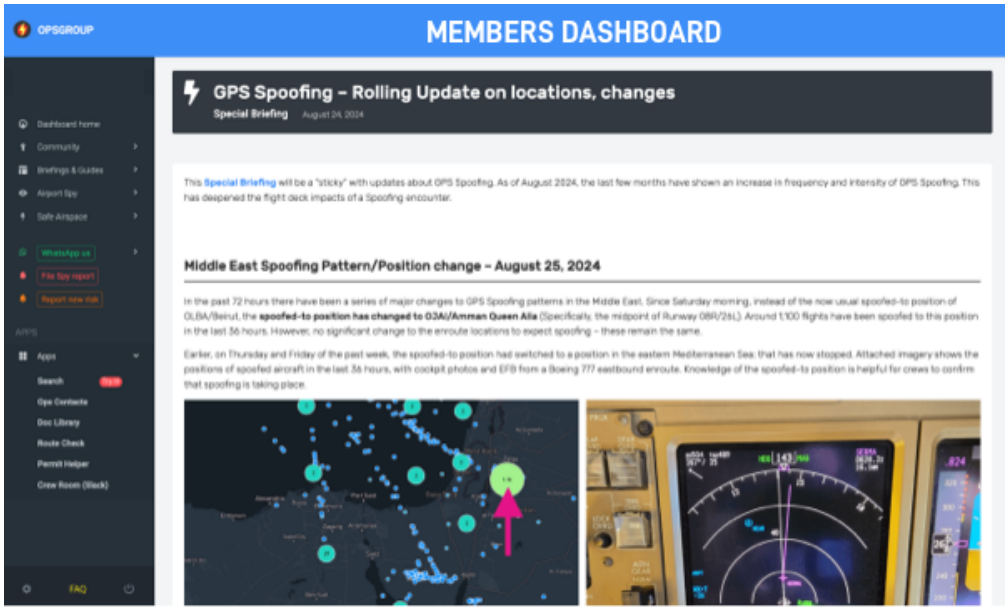
- Why, Where and How GPS Spoofing is happening – full technical details
- Location Maps: Worldwide, Mediterranean, Black Sea, Russia & Baltics, India/Pakistan
- Spoofing statistics and details by FIR
- Aircraft types affected
- Spoofing Patterns
- Changes and current trends



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