

# GPS Jamming & Spoofing

Current Threats and Safety Recommendations



21<sup>st</sup> – 22<sup>nd</sup> January 2025

EASA Headquarters

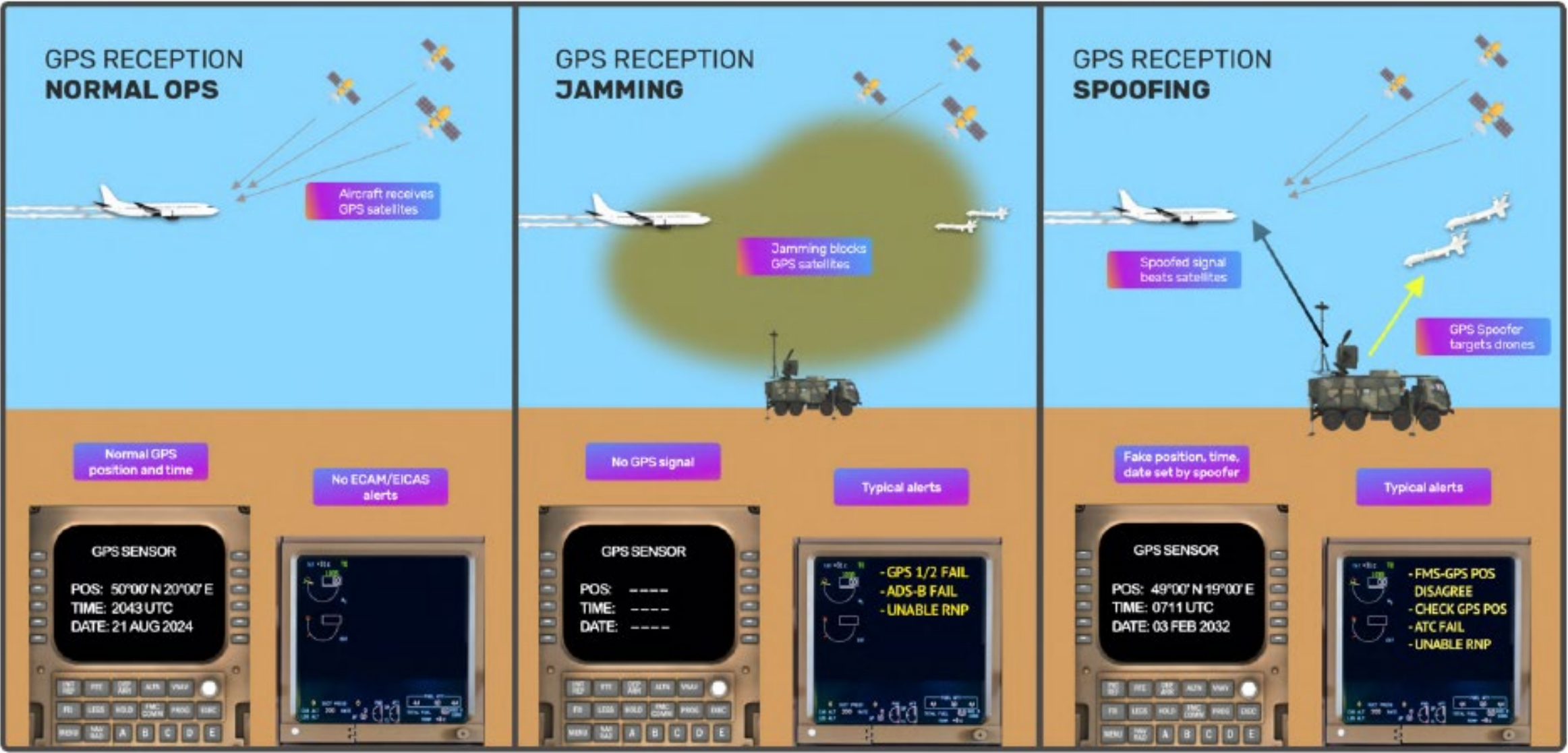
Cologne, Germany

#easabusinessjets



## What are GPS Jamming & Spoofing?

- **Jamming:** Disrupts GPS signal reception.
- **Spoofing:** Introduces false GPS data, tricking aircraft systems.
- **Why it matters:** Impact on flight navigation, critical systems (FMS, GPWS), increasing safety risks in business aviation.

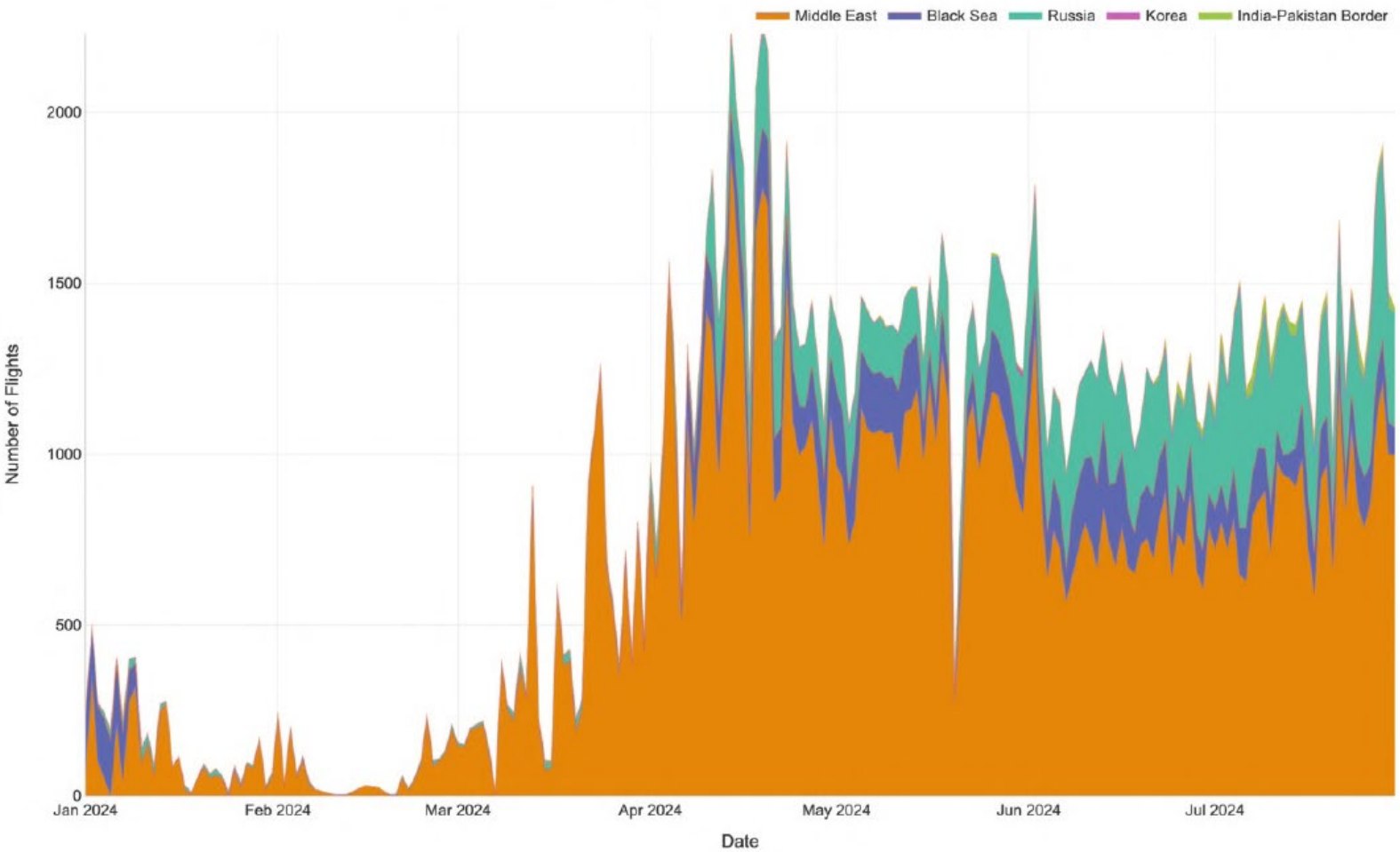




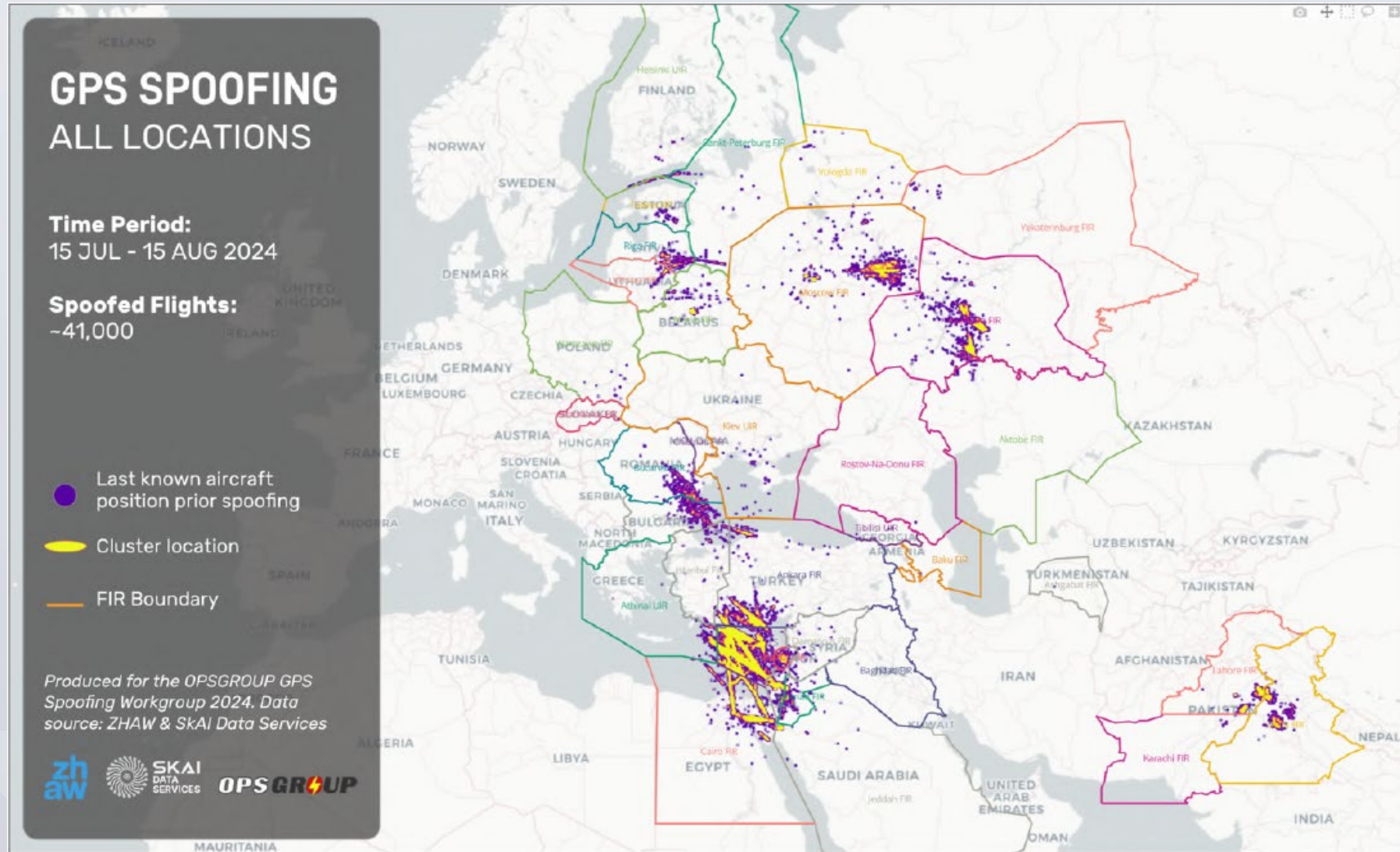
## Massive Spike in Spoofing Events

- 500% increase in spoofing events in 2024.
- From 300 to 1,500 spoofed flights per day.
- Particularly affecting the Eastern Mediterranean, Black Sea, and certain conflict zones.

Daily Estimated Number of Flights Affected by GPS Spoofing by Spoofed-to Region



FIR	COUNTRY	TOTAL FLIGHTS
Nicosia FIR	Cyprus	5655
Tel-Aviv FIR	Israel	3228
Cairo FIR	Egypt	2375
Ankara FIR	Turkey	1195
Samara FIR	Russia	1186
Moscow FIR	Russia	988
Lahore FIR	Pakistan	492
Minsk FIR	Belarus	372
Beirut FIR	Lebanon	371
Delhi FIR	India	316
Sofia FIR	Bulgaria	235
Bucarest FIR	Romania	231
Athens FIR	Greece	193
Amman FIR	Jordan	169
Riga FIR	Latvia	169
Jeddah FIR	Saudi Arabia	115
St. Petersburg FIR	Russia	77
Istanbul FIR	Turkey	67
Tallinn FIR	Estonia	57
Vilnius FIR	Lithuania	51

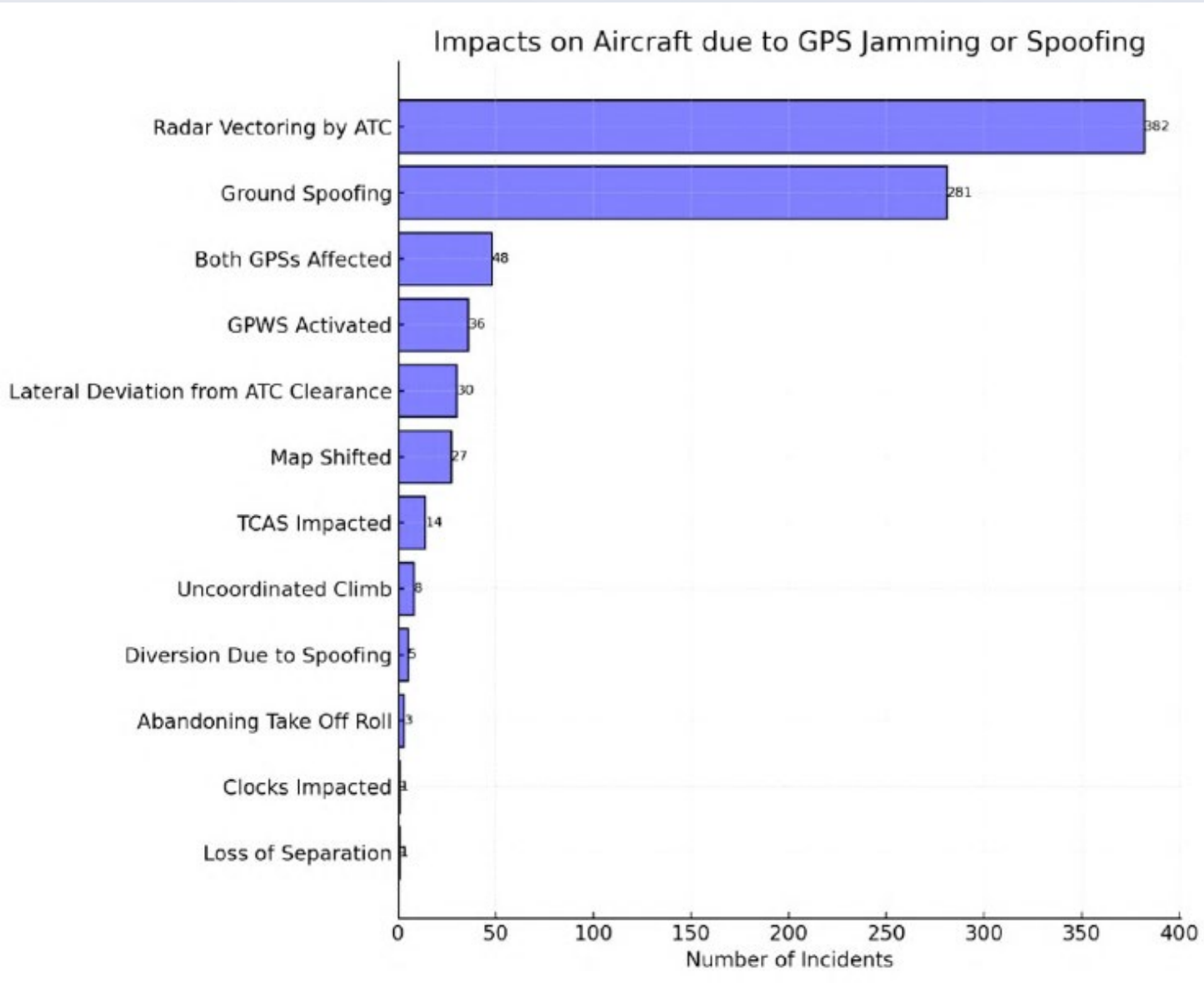


**Map:** All worldwide spoofing locations, August 2024. See Appendix for full map catalogue.

## Critical Systems Affected

- **FMS:** Potential for undetected off-track navigation, increasing risk of entering danger areas or other airspace.
- **GPWS:** Increased risk of Controlled Flight Into Terrain (CFIT) due to false alerts or non-operational system.
- **Weather Radar:** Impacts on detection of convective activity, leading to increased flight into hazardous weather.
- **ADS-B & RNP Operations:** Restricted access to ADS-B required airspace and compromised ability to fly RNP approaches.
- **Aircraft Handling:** Higher workload for crew when managing systems errors and relying on manual procedures.









A depiction of one spoofed aircraft almost entering the Tehran FIR without clearance, close to an active missile base. September 2023.

## Human Factors in GPS Spoofing Incidents

- **Confusion and Cognitive Overload:** Spoofing-induced failures can overwhelm pilots with conflicting system data, impairing decision-making.
- **Startle Effect:** Sudden, unexpected failures in key systems like GPWS can startle flight crews, leading to delayed or incorrect responses.
- **Normalization of Deviance:** Repeated nuisance alerts, especially from GPWS, can desensitize crew to real dangers

## CRM Considerations

- **Team Coordination:** Effective CRM is essential to manage these incidents, ensuring that pilots communicate clearly, distribute workload effectively, and make informed decisions.
- **Fatigue and Stress Management:** Higher-than-usual mental and physical strain when dealing with spoofing or jamming scenarios requires clear strategies to avoid errors due to fatigue.
- **Training Gaps:** The report noted a lack of sufficient technical training on how spoofing affects aircraft systems, which must be addressed



## Key Safety Concerns Raised by OPSGROUP

- 8 overall safety concerns, 33 specific issues.
- Heavy focus on potential CFIT incidents due to degraded GPWS functionality.
- EBAA & IBAC actively involved in the workgroup, contributing to the safety focus and mitigation strategies



## Short-term Solutions

- **Crew Training and Awareness:** Immediate awareness of spoofing-prone areas.
- **Operational Procedures:** Updated SOPs for recovery from GPS loss or spoofing events.
- **Backup Navigation Systems:** Enhanced reliance on ground-based navaids during GPS outages.

## Long-term Considerations

- GPS hardware and software updates to detect and mitigate spoofing.
- Exploration of alternative satellite navigation systems

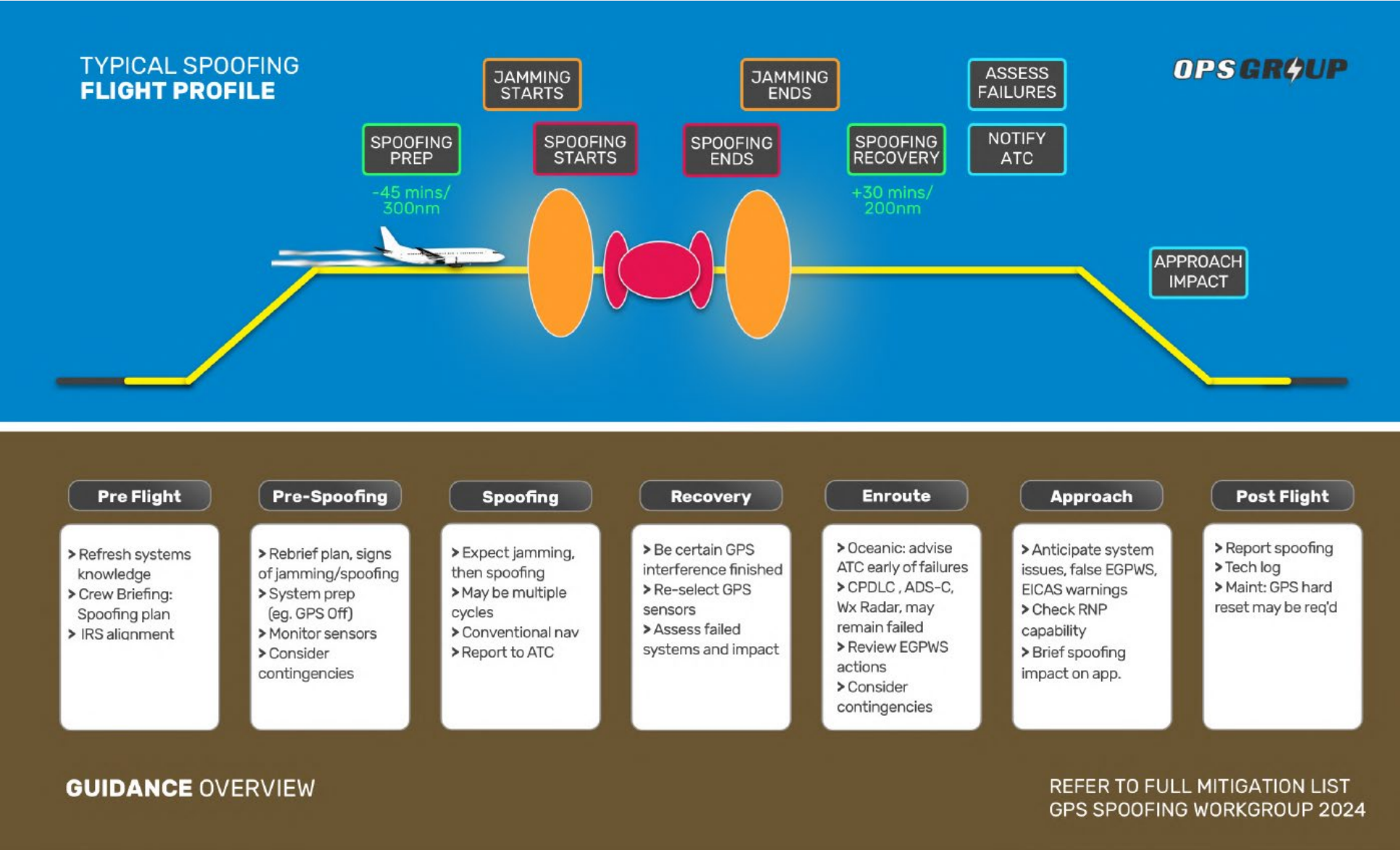
## Immediate Actions

- **Pre-flight Risk Assessments:** Ensure crews are briefed on high-risk areas for GPS jamming and spoofing (e.g., Eastern Mediterranean, Black Sea).
- **Procedure Updates:** Incorporate clear, simple steps to deal with potential spoofing scenarios, ensuring proper use of alternative navigation tools (e.g., ground-based navaids).
- **Enhanced CRM Training:** Focus on team coordination, communication, and effective



## Long-term Strategies

- **Improved Avionics and Systems:** Work with manufacturers to integrate spoofing detection into avionics systems.
- **Industry-Wide CRM Enhancements:** Advocate for standardized CRM protocols across business aviation to manage GPS spoofing threats, emphasizing stress management, communication, and teamwork during high-pressure situations.
- **Continued Use of Conventional Navigation Aids:** Maintain a strong backup network of ground-based navigation aids to minimize reliance on GPS



## Importance of Safety Culture

- **Proactive Awareness:** Foster a safety culture where pilots and operators remain vigilant and prepared for spoofing events.
- **Normalization of Risk:** Combat the growing risk of crews becoming desensitized to spoofing-induced system failures. Encourage proactive reporting of incidents and concerns.
- **Fatigue Risk Management:** Ensure that operators have programs in place to mitigate fatigue-related risks, which can be exacerbated by the higher workload and stress associated with handling spoofing events.



## Key Issues

- **False System Recovery:** GPS receivers may appear normal after spoofing, but can still be corrupted, posing long-term risks.
- **Reset Procedures:** Ensure that crews understand the importance of full system resets after a spoofing event, especially when entering sensitive airspace or critical phases of flight.
- **Trust in Automation:** Spoofing can erode pilots' trust in their systems, particularly when previously reliable systems like GPWS or ADS-B are compromised. This requires psychological resilience and strong CRM to navigate the post-event confusion

## FINAL

### OF THE GPS S

Fli

**OPS GROUP**

## GPS S



Typical spoofing flight profile

**OPS GROUP**

## Extract GPS Spoofing

# GPS SPOOFING



### Current trends and changes

**OPS GROUP**

Extract from the report of the  
**GPS Spoofing WorkGroup 2024**



**Thank you for your attention!**

[safety@ebaa.org](mailto:safety@ebaa.org)

[mwauters@ebaa.org](mailto:mwauters@ebaa.org)