

Global Navigation Satellite System (GNSS) Vulnerabilities: From Jamming to Spoofing

Gian Andrea Bandieri

WORC 2024

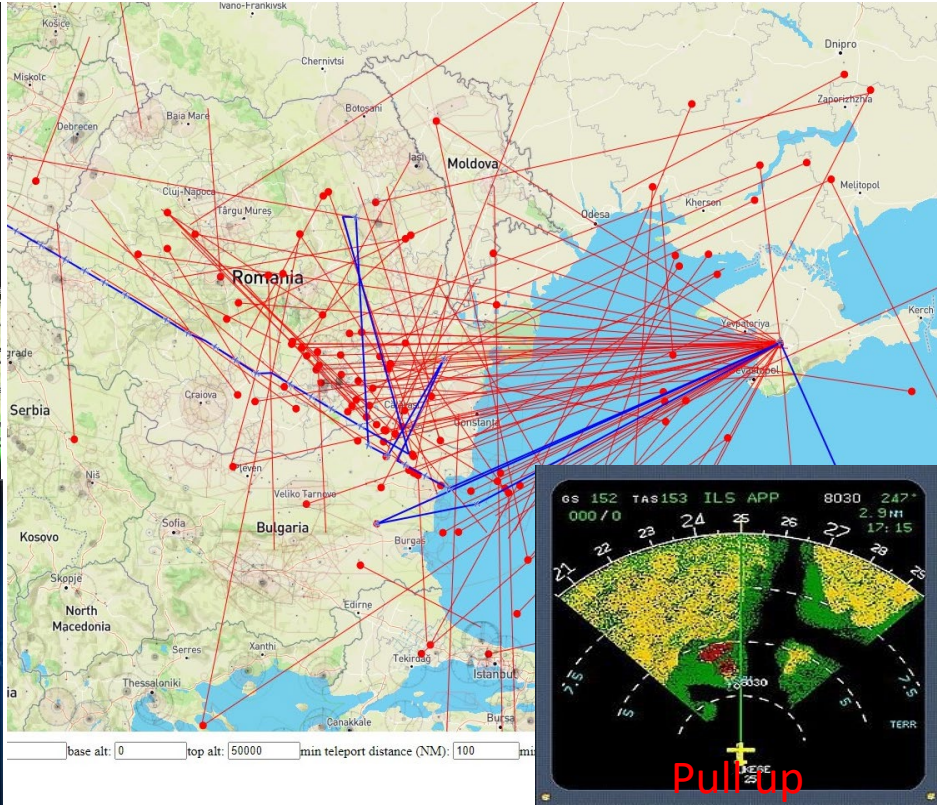
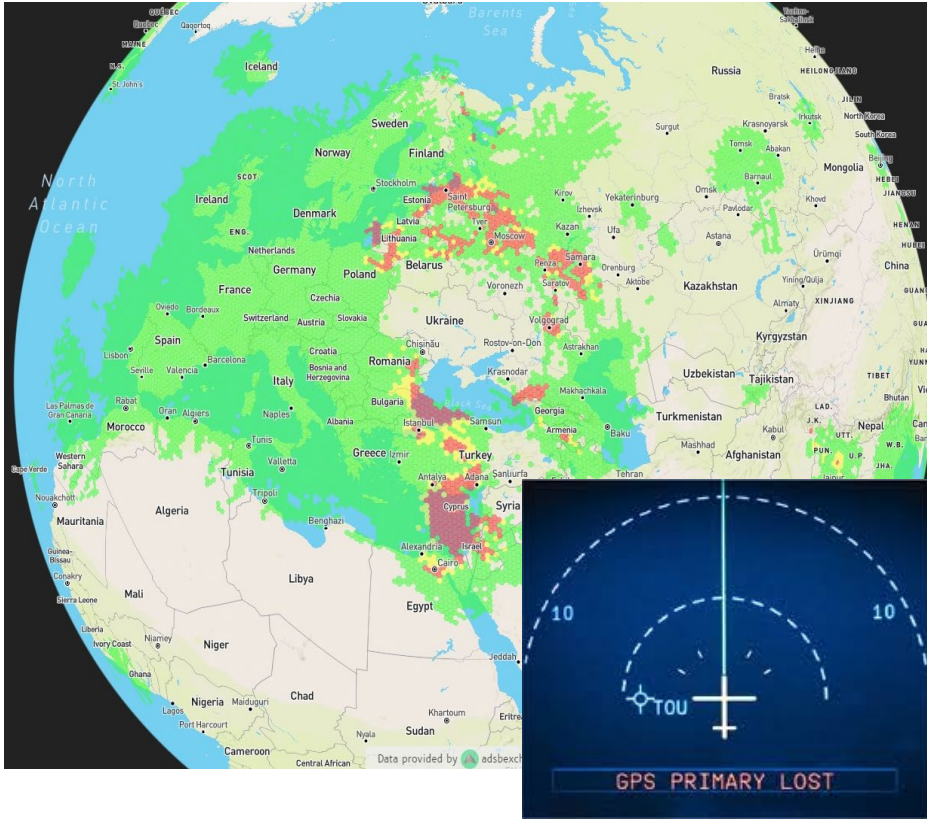
Warsaw, 3 July 2024

Your safety is our mission.

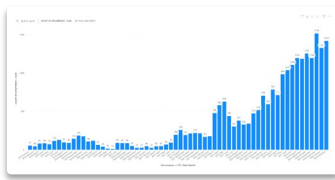
TLP:AMBER+STRICT sharing restricted
to the recipient *organization* only.

An Agency of the European Union 

GNSS Robustness issue



Evolution



August 2023



January 2024



May 2024

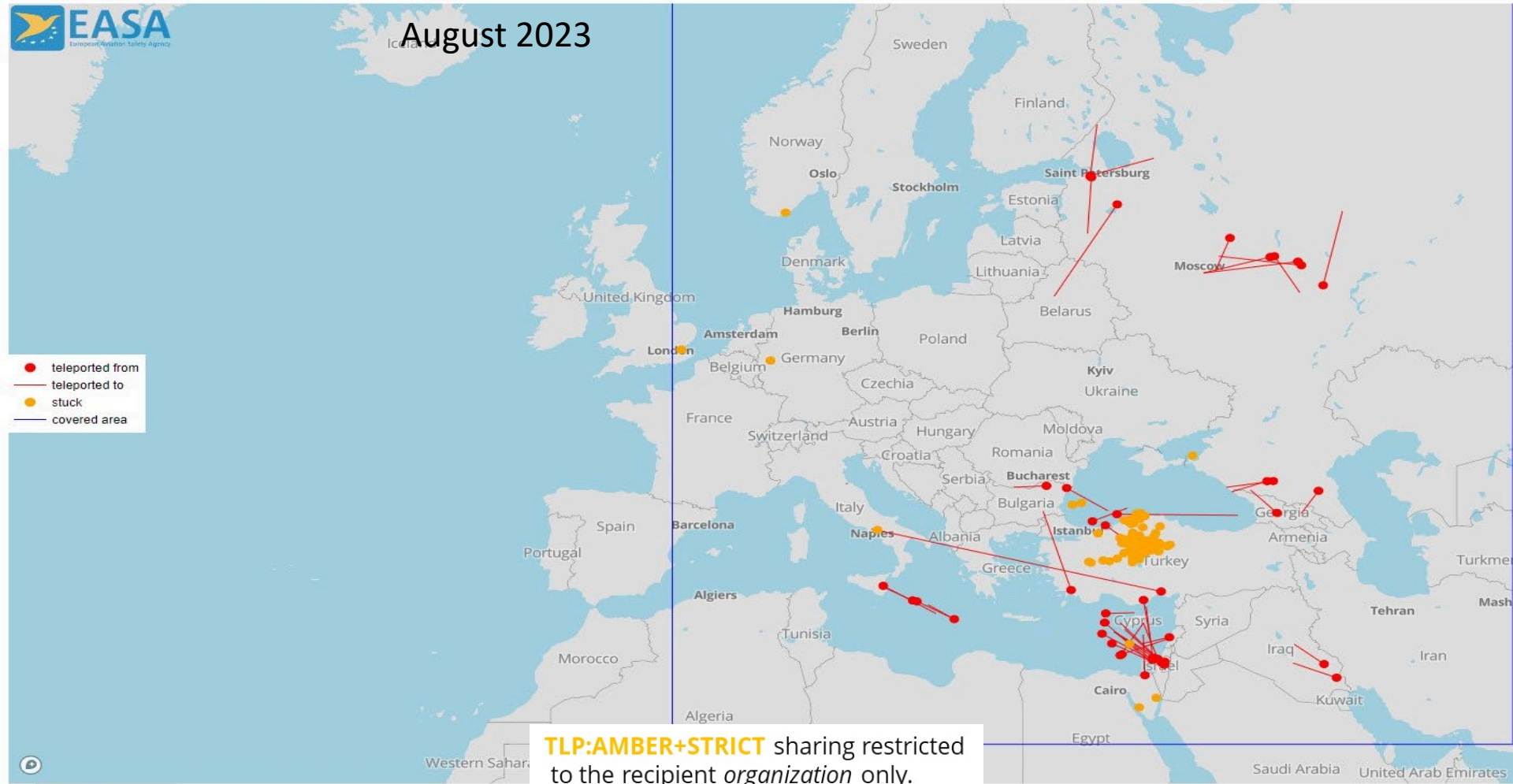


Area with low altitude spoofing



August 2023

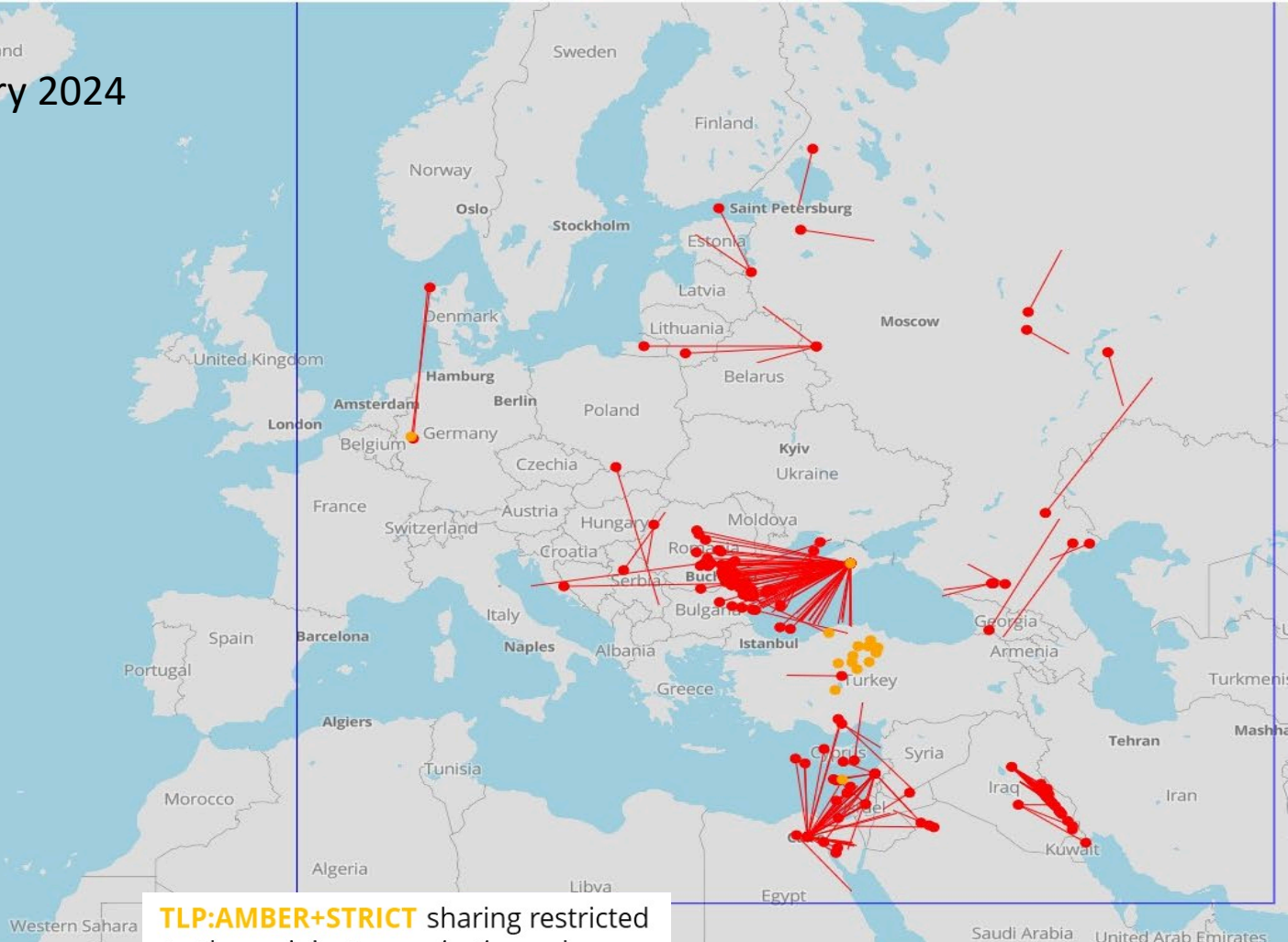
- teleported from
- teleported to
- stuck
- covered area



TLP:AMBER+STRICT sharing restricted to the recipient *organization* only.

Iceland
January 2024

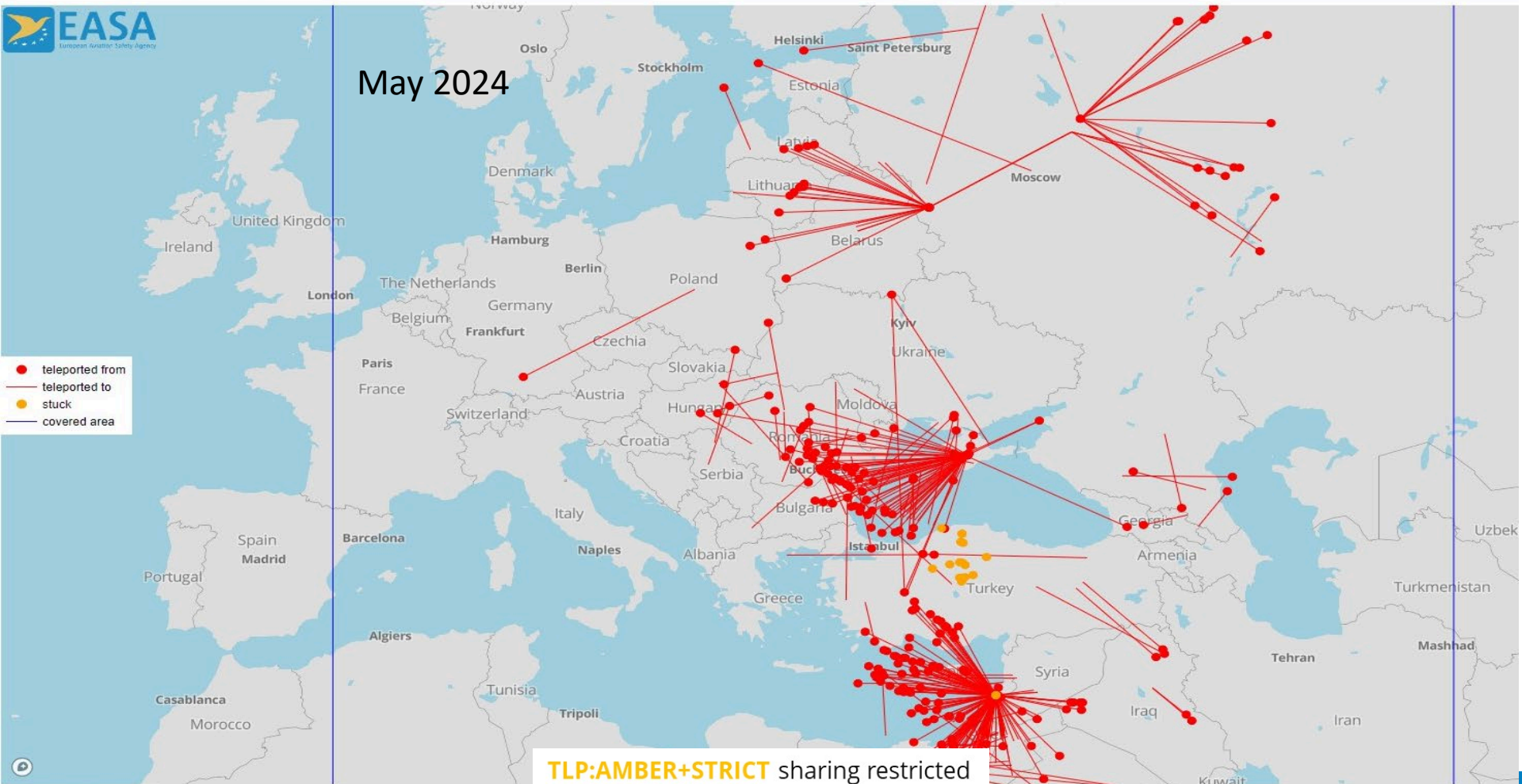
- teleported from
- teleported to
- stuck
- covered area



TLP:AMBER+STRICT sharing restricted to the recipient *organization* only.

May 2024

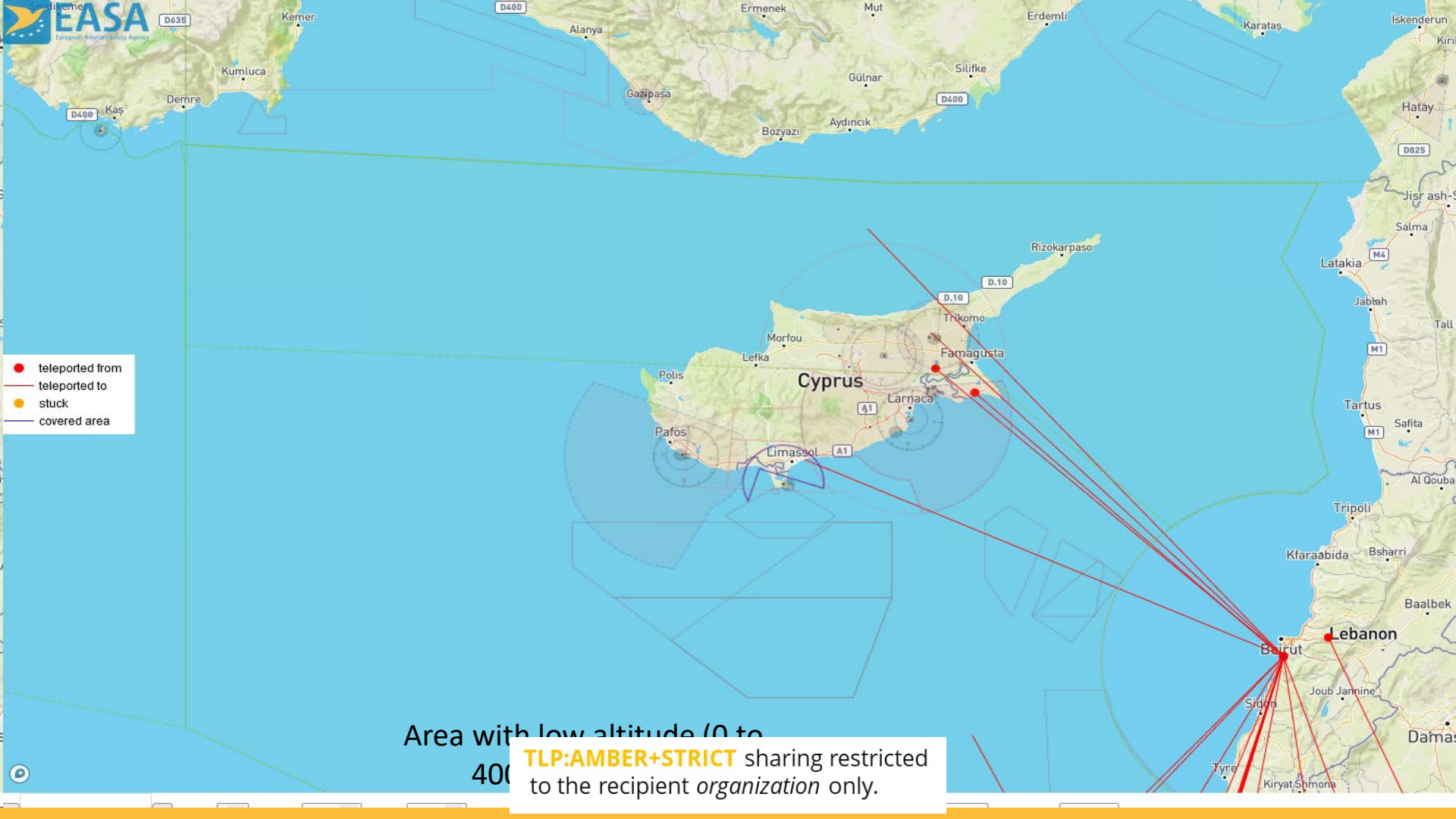
- teleported from
- teleported to
- stuck
- covered area



TLP:AMBER+STRICT sharing restricted to the recipient *organization* only.

in stuck duration (s): 30 search reg: search hex:

< 05/01/2024 > nac_p: 7 base alt: 0



GNSS interference: safety or security issue?

- Intentional action
- Most likely, the effect of Electronic Warfare (EW)
- Civil aviation not the primary target



What is EASA doing (safety side)

2022

2023

2024

2025

...

Monitoring and analysis of events

Short term (containment)

- Understanding the situation
- Provide recommendations
- Increase awareness

SIB 2022-02
Rev.3 in
preparation

Medium term (corrective)

- Comprehensive risk assessment
- Impact of PBN regulation

Amendment of
the PBN-IR

Long term (planning)

- Ensure sufficient coverage of complementary navigation means
- Best Intervention Strategy

Support to MON
definition

SIB 2022-02 Revision 3

1. New type of events reported:

- spoofing during departure and arrival procedures,
- uncoordinated high rate of climb in reaction to spurious alerts of terrain and traffic collision avoidance systems

→ spurious traffic collision avoidance system alerts

2. Stressing that spoofing is riskier than jamming.

3. FIRs updated

4. Recommendations updated

→ In some cases, the risk has increased. However, an unsafe condition is not confirmed at this stage

Monitoring the situation – recent events

Baltic states

- FINNAIR temporarily stopped operation at TARTU (EETU)
 - TARTU is for GNSS capable aircraft only. No backup available
 - FINNAIR will resume operation as soon as alternative means is available
 - For EASA it is not an unsafe situation. 2 flights diverted to an alternate destination resilient to GNSS outages

East Mediterranean Sea

- increase of GPS spoofing occurrences with impacts on aircraft performance are recorded since December 2023
- Contrarily to other regions, spoofing is active during low altitude operations (STARs, approaches, landing, taxi, takeoff, SIDs)
- Unpredictable aircraft behaviors are recorded:
 - Aircraft difficulties to fly conventionally (i.e. non GNSS)
 - Deviation from SIDs and STARs
- Aircraft deviation from ATC clearance
- Aircraft reporting numerous systems malfunctions (Clock, Fuel, FMS, Map Shift, TAWS, TCAS)
 - Aircraft uncoordinated climbs in response to TAWS alerts with very high rates of climb
 - Misleading TCAS (TAs), rare but

Is that all?

- GNSS interference is the evident effect of Electronic Warfare on civil aviation
- Probably there might be additional effects due to EW, not fully known today
- Symptoms being occasionally noted:
 - Latching effect on receivers → INOP
 - Other systems showing spurious alerts: EGPWS, TCAS, ...
- The full impact of EW on aircraft systems is yet to be fully understood..