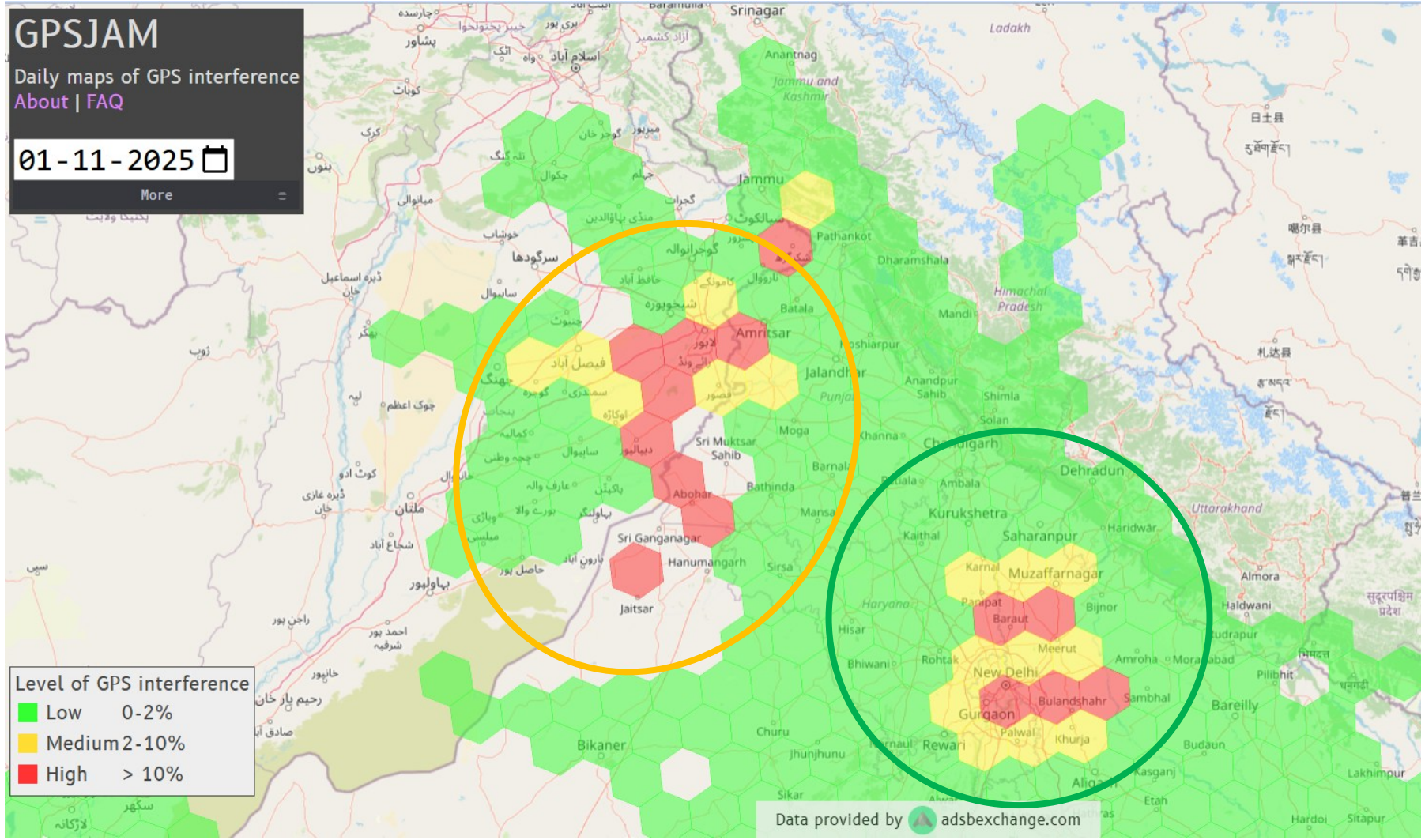
RECENT NEWS!

References: https://www.thehindu.com/news/national/why-was-there-a-tech-glitch-at-delhi-airport-explained/article70284947.ece
https://www.thehindu.com/sci-tech/technology/what-are-the-threats-from-gnss-spoofing-explained/article70284960.ece
https://www.lokmattimes.com/mumbai/mumbai-airspace-under-notam-alert-as-india-warns-of-possible-gps-signal-interference-from-nov-13-to-17-a525/

IP-based AMSS Glitch and GNSS Spoofing at Delhi Airport

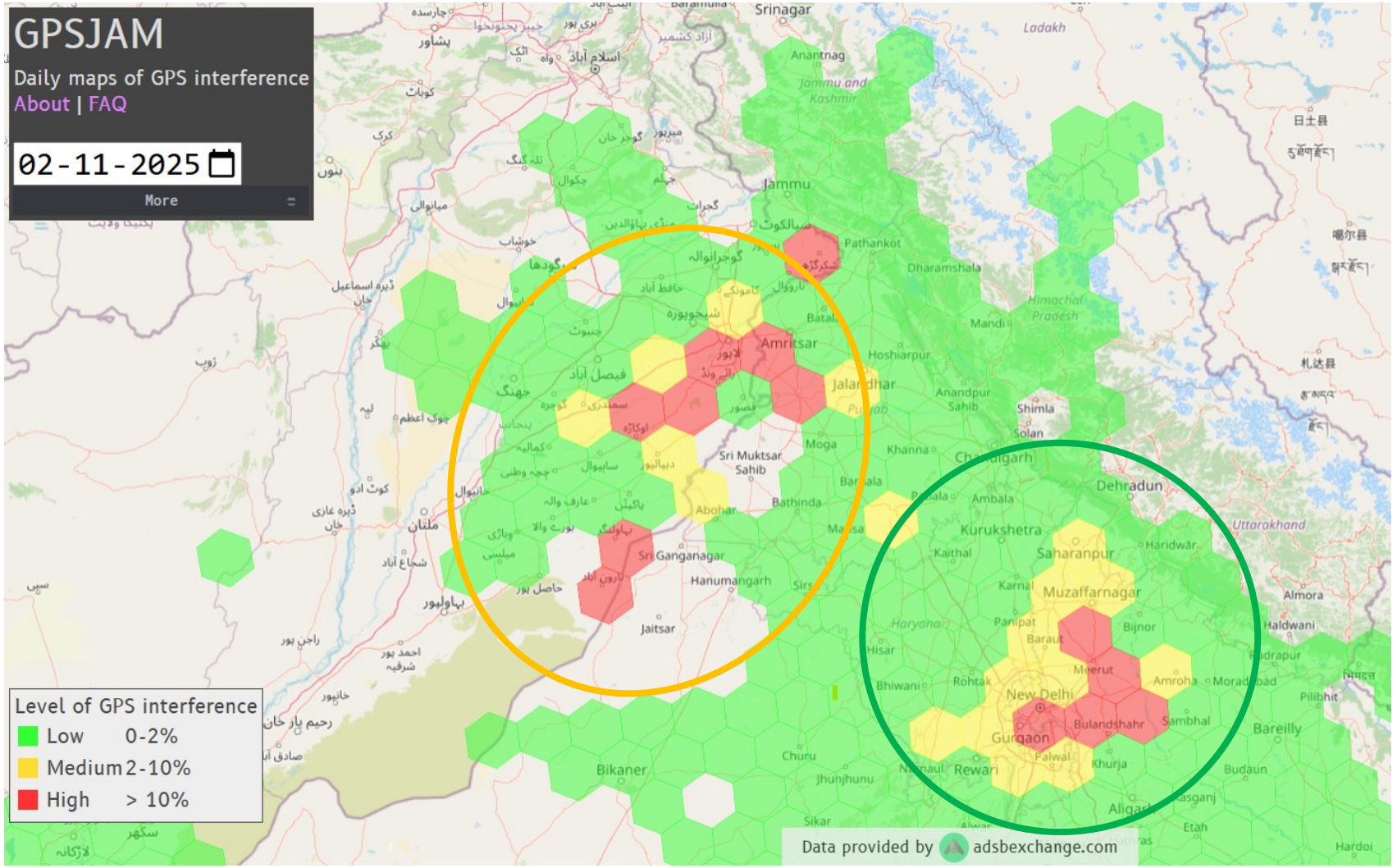
- Automatic Message Switching System (AMSS) is a core communication backbone in air traffic management.
- Primary reason for AMSS glitch at Delhi Airport (6 Nov 2025) is the synchronization breakdown between the AMSS servers.
- Other reason for AMSS glitch can be co-existence of old and new systems that is vulnerable to cyber threats.
- GNSS spoofing reported in the first week of November in Delhi Flight Information Region (FIR).
- DGCA issued an advisory (11 Nov 2025) to report any GNSS spoofing within 10 min of its occurrence.
- Notice To Airmen (NOTAM) issued (13-17 Nov 2025) in Mumbai FIR to ensure airlines are prepared for potential GNSS disruptions.

India-Pakistan Border and Delhi GNSS Spoofing Map



References: https://gpsjam.org/

India-Pakistan Border and Delhi GNSS Spoofing Map



References: https://gpsjam.org/

GNSS spoofing at Delhi is highly concerning.

GNSS/GPS Spoofing

Global Navigation Satellite System (GNSS)

What is GNSS?

- GNSS is a Radio-frequency (RF) signal broadcasted by the group of satellites.
- The user's GNSS receiver receives this RF signal and calculates it's position, navigation, and timing (PNT) data.
- Users are civilians, research personnels, aircrafts, drones, military units, etc.

- India's NavIC, Russia's GLONASS, China's BeiDou, Europe's Galileo, and USA's GPS.
- Navigation with Indian Constellation (NavIC) provides 2 services:

1. Standard Position Service (SPS), no encryption.
2. Restricted Service (RS), with encryption.
3. Bands with carrier frequency L1-1575.42 MHz, L5-1176.45 MHz, and S-2492.028 MHz

References: https://www.isro.gov.in/media_isro/pdf/SateliteNavigation/Draft_NavIC_SPS_ICD_L1_Oct_2022.pdf

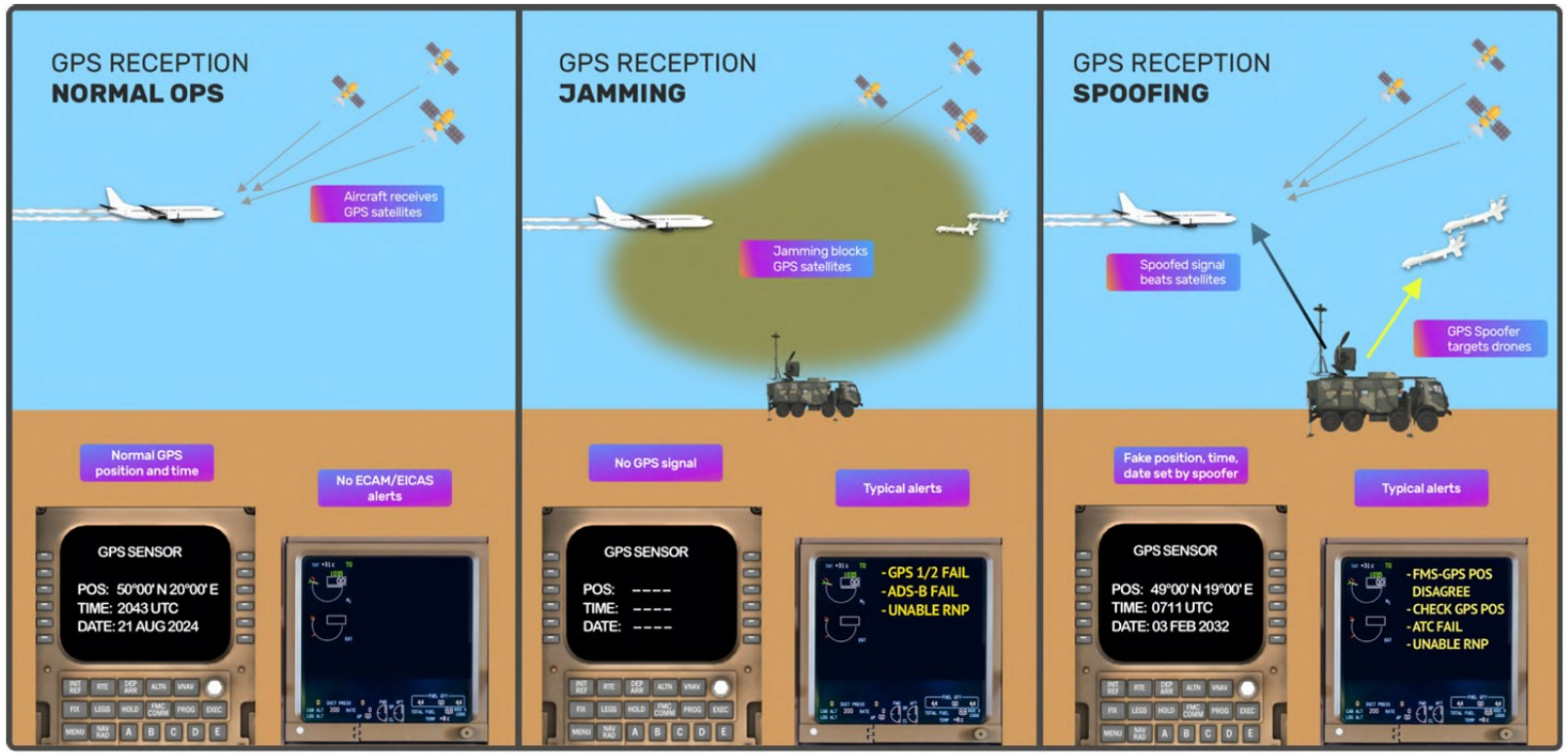
What is GNSS Spoofing?

- **Jamming**

1. Ground-based radio transmitter transmits noise on the GNSS frequency band(s).
2. As a result, the GNSS receiver loses the low power satellite signal.

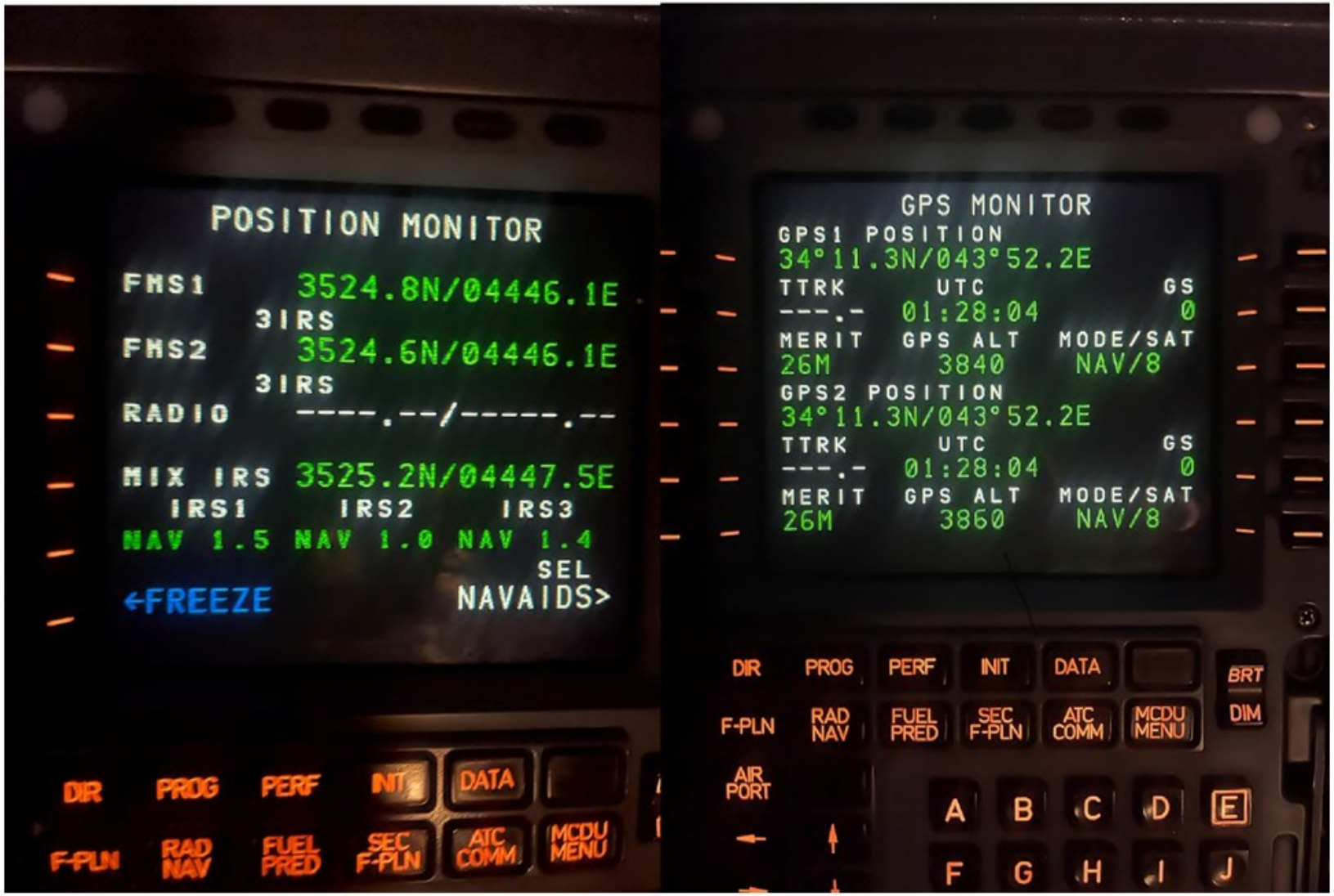
- **Spoofing**

1. Another ground-based radio transmitter begins to send a high power fake GNSS signal.
2. The GNSS receiver accepts this fake signal and calculates incorrect position, time, and altitude.



GPS Reception during normal ops, jamming, and spoofing. Larger version in Appendix. Image source: OPSGROUP.

References: https://ops.group/blog/gps-spoofing-final-report/



An example of GPS Spoofing in action during cruise phase: FMS position shows correct, GPS is being spoofed. Note also GPS Altitude incorrect, True track (TTRK) and Ground Speed (GS) values are zero - all indications of spoofing. A320, ORBB FIR.

References: https://ops.group/blog/gps-spoofing-final-report/

GNSS Spoofing Equipment

- GNSS spoofing is carried out by large-scale military Electromagnetic Warfare (EW) equipment.
- Example: SAMYUKTA is an integrated EW system for the Indian Army.

References: https://www.tataadvancedsystems.com/electronic-warfare-systems

Why and Where GNSS Spoofing is happening?

- GNSS Spoofing is a very effective mechanism to counter hostile drones and disturbing the flight path of GPS-guided missiles.
- The primary actors carrying out spoofing are military units.
- **Spoofing signal is affecting the civil aircraft in the conflict regions e.g. Middle East, Western Russia, and India-Pakistan border.**

References: https://ops.group/blog/gps-spoofing-final-report/

Effects of GNSS spoofing

- Spoofing cause GNSS receiver to calculate incorrect navigation results even after it leaves the spoofing area. This will continue until the receiver is manually reset or the navigation data expires.
- Unplanned entry into danger areas, restricted airspace, and other FIRs.
- Wrong runway selection or risk of landing on closed runway.
- Increased crew and Air Traffic Control (ATC) workload.
- Severe impact on Enhanced Ground Proximity Warning Systems (EGPWS).
- Automatic Dependent Surveillance-Broadcast (ADS-B) may either completely stop working or sends false PNT information to the ATC and other aircrafts.

References: https://ops.group/blog/gps-spoofing-final-report/

Solutions for combating GNSS spoofing

- Short term solutions are:

1. Relying on Inertial Reference System (IRS) up to 5 hours if GNSS receiver fails.
2. Crew (aircrafts and ATCs) awareness, guidance, and training on how to handle safe landing of aircraft.

References: https://ops.group/blog/gps-spoofing-final-report/
https://www.thehindu.com/sci-tech/technology/what-are-the-threats-from-gnss-spoofing-explained/article70284960.ece

Solutions for combating GNSS spoofing

- Long term solutions are:

1. A live GPS jamming and Spoofing map
2. In-flight resets
3. Using Enhanced Long Range Navigation (eLoran): Land-based transmitters with high-power low frequency signals (other than GNSS frequency band) providing PNT services
4. Avionics improvements via
    1. software e.g. on board spoofing detection and alerting
    2. hardware e.g. using Controlled Reception Pattern Antenna (CRPA)
5. Using quantum sensors and atomic clocks for precise PNT services
6. Encryption and Authentication

References: https://www.gpsworld.com/eloran-part-of-the-solution-to-gnss-vulnerability/
https://ops.group/blog/gps-spoofing-final-report/
https://www.gpsworld.com/innovation-getting-there-safely-with-chip-scale-atomic-clocks/

Is the incident at Delhi Airport deliberate Jamming/Spoofing, Testing, or Spillover?

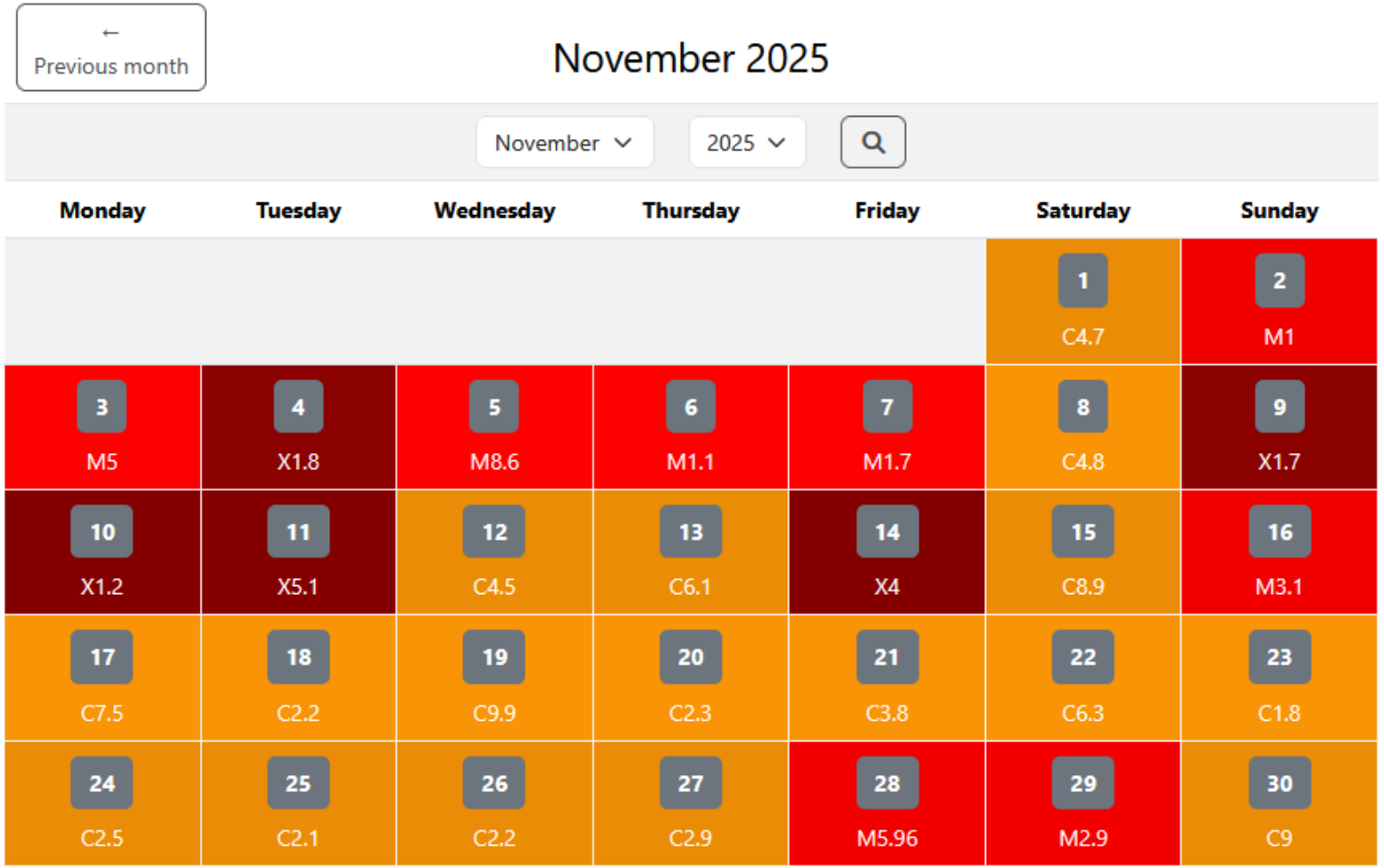
The source of interference is unknown but there can be three possibilities:

1. India may be stress testing EW resilience during its ongoing integrated exercises. (But no NOTAM was issued)
2. Cross-border EW could be affecting Indian FIRs-intentionally or accidently.
3. Large, high-powered shipborne radars and jammers from regional navies often bleed into civilian airspace systems.

The incident can be likely a live electromagnetic contest, where each side across borders tests limits, probes defences, and prepares for future contingencies.

References: https://idrw.org/india-issues-gps-interference-notam-over-mumbai-fir-a-major-signal-that-the-electromagnetic-battle-has-begun/

Solar Flares?



References: https://www.spaceweatherlive.com/en/archive/2025/11.html