# Technical Guide

## GPS SPOOFING


- Spoofing: Why, Where and How
- Location Maps and description by FIR
- Current trends and changes

OPS GROUP

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

# GPS Spoofing

# Why, where, how.

**GPS spoofing** began to severely impact civil aviation in September 2023. Even though GPS interference is not a new phenomenon, the scale and effects of the current wave of spoofing are unprecedented.

In the first few months, relatively few aircraft were affected, but by January 2024, an average of 300 flights a day were being spoofed. By August 2024, this had grown to around 1500 flights per day.

**Most recently, for the one month period from July 15 - August 15, 2024, a total of 41,000 flights experienced spoofing.**

Because modern aircraft have incorporated GPS into a large number of aircraft systems, the impact of a spoofed GPS signal has had severe and cascading effects. These include the FMS, Hybrid IRS, the aircraft clock, GPWS, Weather Radar, CPDLC, ADS-B and ADS-C, as well as numerous other systems.

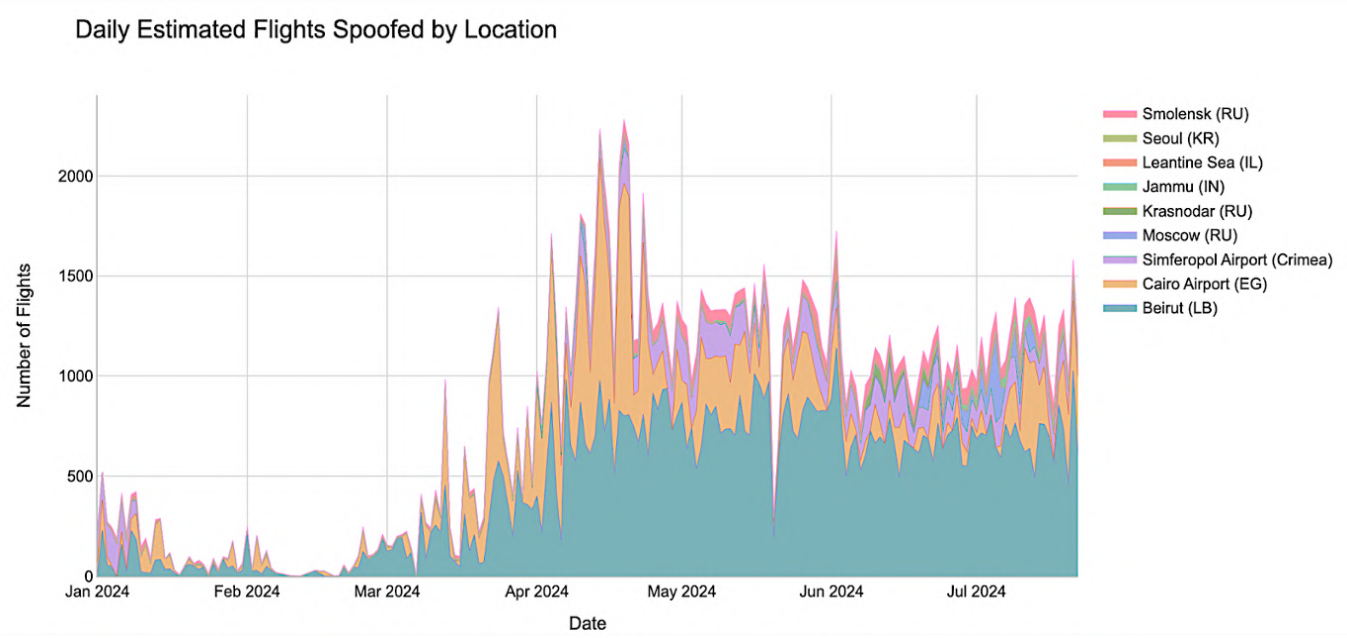
**This section of the report will provide a technical overview of the reasons for spoofing, methodology, locations, and current trend.**

# Major increase in spoofing in 2024

This chart shows the daily number of estimated spoofed flights per falsified location.

A clear rise in spoofing incidents is evident from April 2024 onwards, based on ADS-B data. Not all spoofing can be detected this way; the true number could be significantly higher.

**Data source: ZHAW/SkAI Data Services, using the OpenSky Network.**



# Why is GPS Spoofing happening?

Almost all current GPS spoofing incidents currently affecting civil aircraft are related to conflict zones.

Spoofing is a very effective mechanism to counter drones, which are increasingly used in modern warfare. Spoofing platforms and devices are operated by military units.

These signals used to counter drones, and disrupt/confuse other GPS receivers, are also being picked up by civil aircraft.

**There is no evidence, so far, to suggest that civil aircraft are being deliberately targeted.**

## Primary actors currently carrying out GPS Spoofing

- Military units targeting hostile drones, and drone swarms, in conflict zones (e.g. Israel, Ukraine, Russia).
- Military units acting on behalf of the state, disrupting shipping (e.g., Crimea, Black Sea)
- Military units disturbing the flight path of other GPS-guided ammunition, missiles, or vehicles (autonomous or manned).

## Other actors

- Police, Public Safety and National Security agencies preventing drone use at events (e.g., Euro 2024, Olympics), borders, and sensitive areas. They often use counter-drone systems to jam or spoof GPS to force drones to land.
- Commercial drivers (truck, taxi) may use jamming or spoofing to interfere with their reported locations, but there is no verified impact on civil aviation from these.

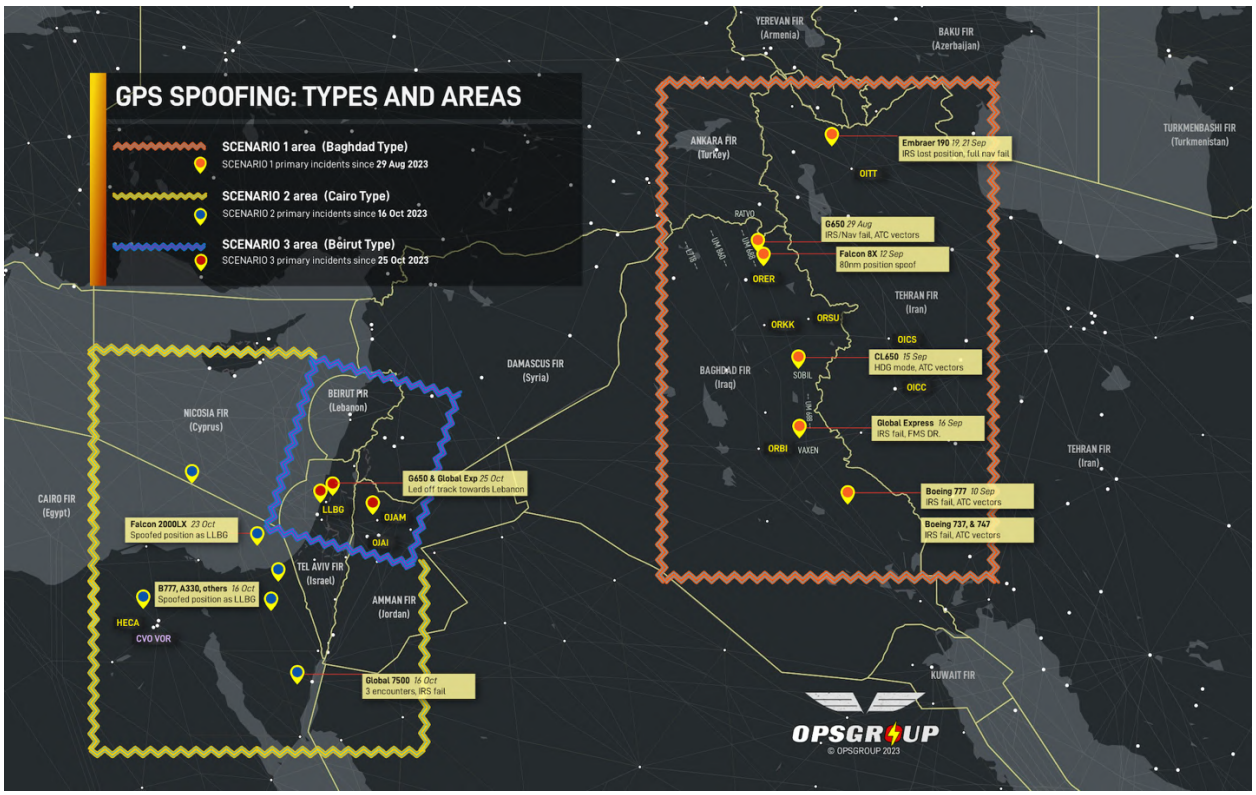
# Where is GPS Spoofing happening?

GPS Spoofing is currently concentrated in **very specific areas near conflict zones**. The highest level of spoofing is in the eastern Mediterranean, near Israel, Lebanon, Cyprus and Egypt. Other areas of significant spoofing include the Black Sea, western Russia, and the India/Pakistan border. Complete maps are shown in the next section.

## History and Locations

The first series of GPS Spoofing events took place in September 2023 in the area of northern Iraq, centered on Baghdad. Approximately 20 aircraft reports were received by OPSGROUP, with similar patterns of system behavior: navigation position uncertainty, FMS degradation, apparent IRS failures. Some aircraft were left unable to navigate independently after the spoofing event, requiring ATC vectors. Aircraft clocks were showing wrong times.

By November 2023, 50 reports had been received by OPSGROUP with further spoofing locations being noted in the Eastern Mediterranean, centered on Cairo, Tel Aviv and Beirut.




Initial GPS Spoofing locations, as at November 2023. Source: OPSGROUP.

During 2024, as employment of spoofing tactics by military forces widened, new spoofing locations were identified in the Black Sea region, western Russia and the Baltics, North/South Korea border areas, western Ukraine, and the India/Pakistan border.

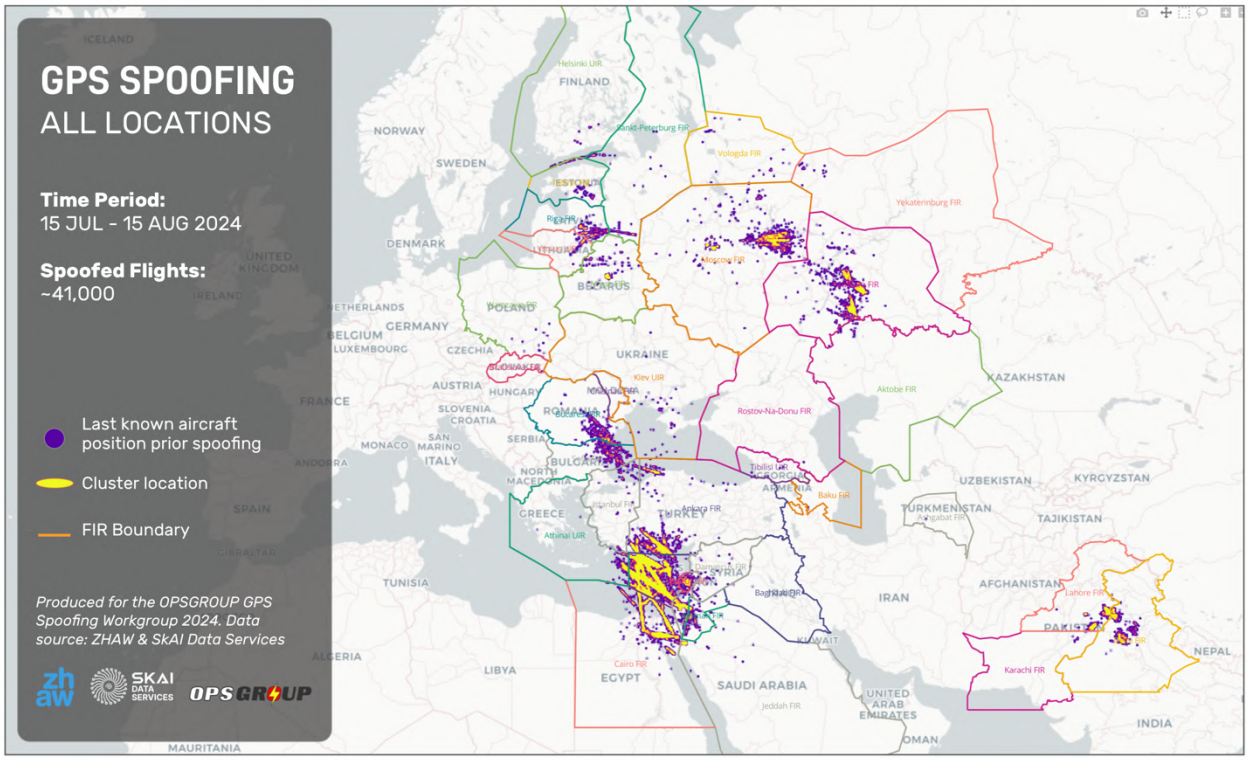
## Spoofing by Flight Information Region (FIR)

The table below shows the number of aircraft impacted by spoofing in the Top 20 FIR's affected, during the period July 15 – August 15.

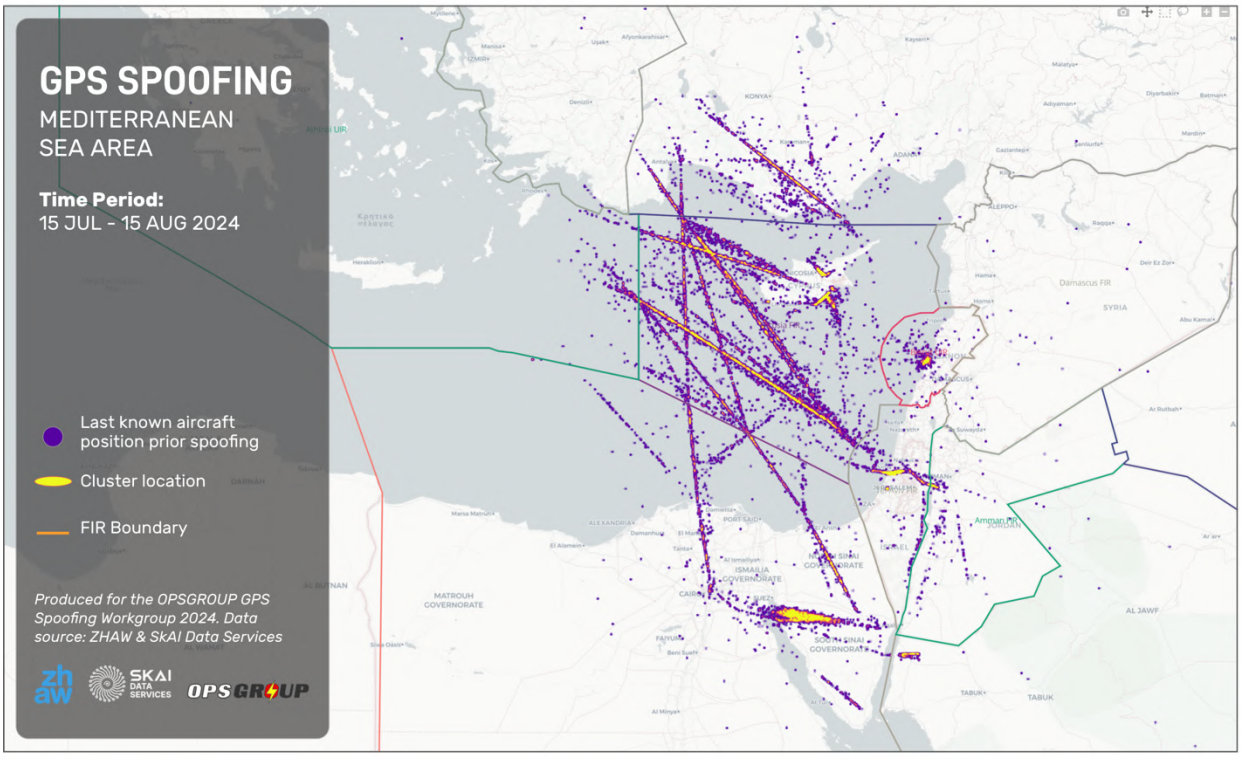
| FIR | COUNTRY | TOTAL FLIGHTS |
|---|---|---|
| **Nicosia FIR** | Cyprus | **5655** |
| **Tel-Aviv FIR** | Israel | **3228** |
| **Cairo FIR** | Egpyt | **2375** |
| **Ankara FIR** | Turkey | **1195** |
| **Samara FIR** | Russia | **1186** |
| **Moscow FIR** | Russia | **988** |
| **Lahore FIR** | 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** |

**Table:** Number of spoofed flights by Flight Information Region (FIR), taken from data for the period July 15 - August 15, based on last known position before spoofing. Note that not all flights can be traced to a last known position due to GPS Jamming preceding the spoofing event. Only 17,000 of the 41,000 flights spoofed in this period are included in this data. However, the data does give a good representation of the most affected FIR's. Source: ZHAW/SkAI Data Services.

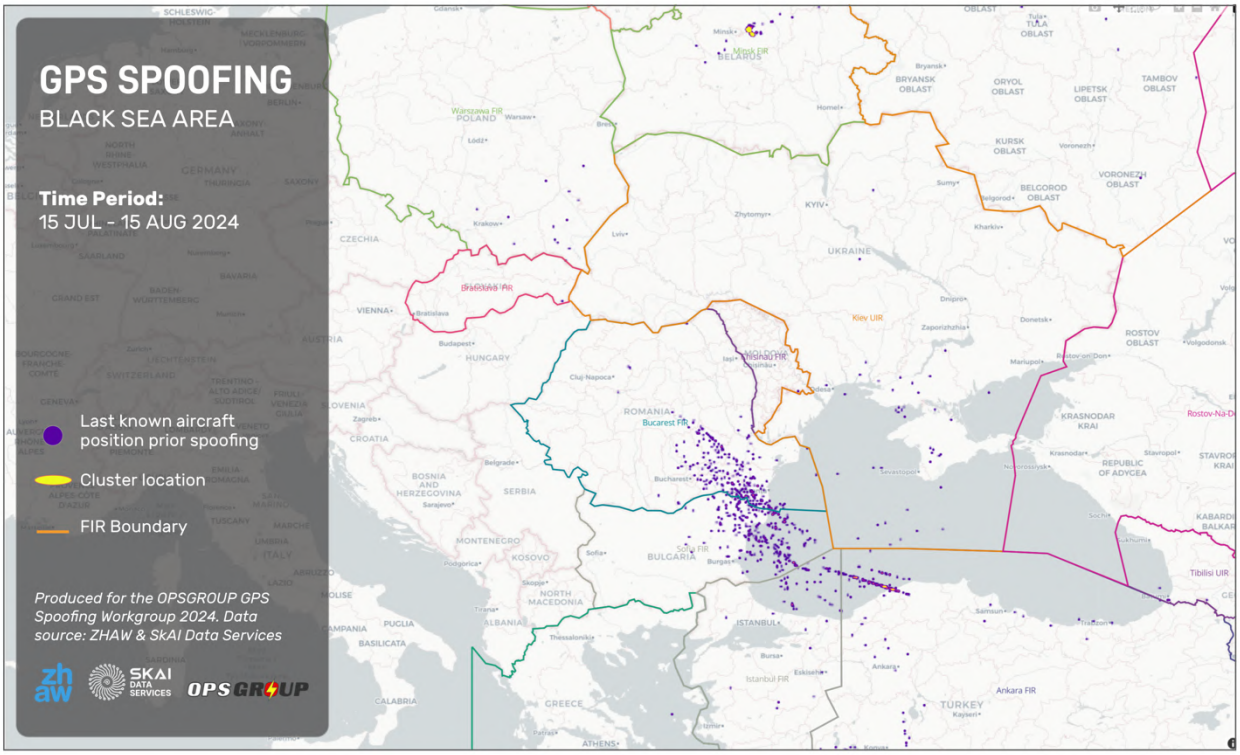
# Location Maps



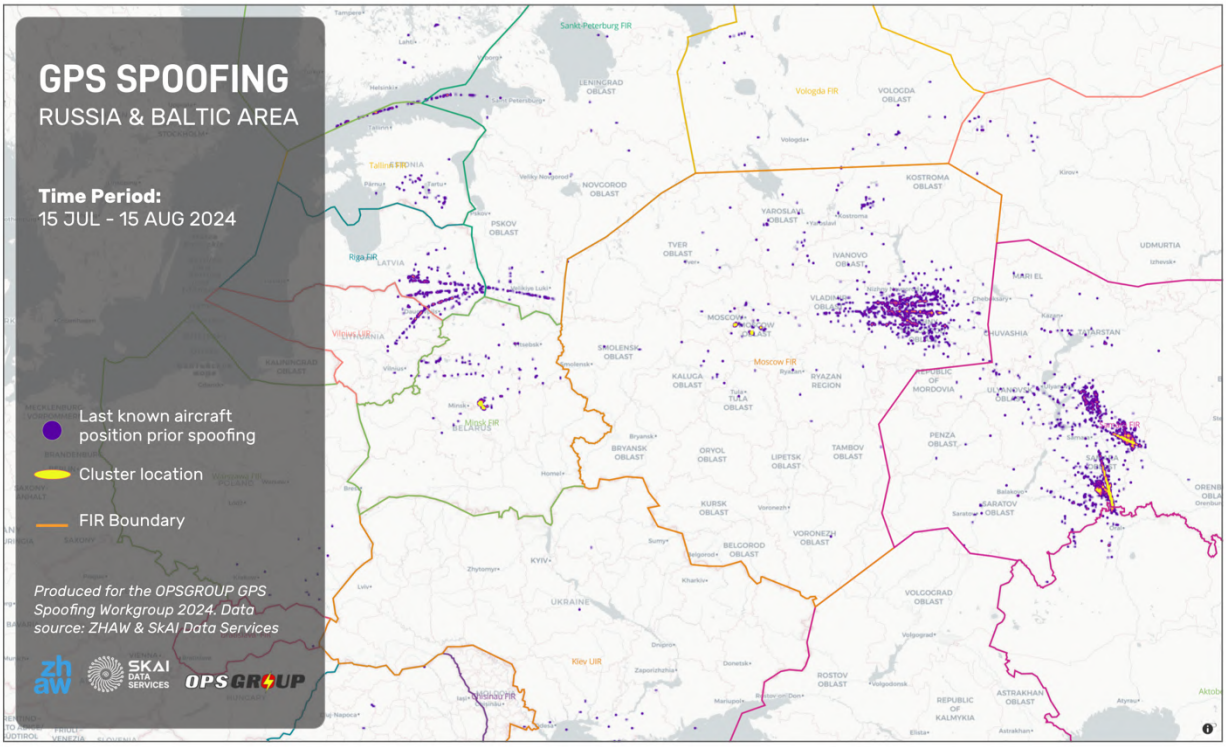

**Map:** All worldwide spoofing locations, August 2024. See Appendix for full map catalogue.




**Map:** Mediterranean Sea area, August 2024. See Appendix for full map catalogue.




**Map:** Black Sea area, August 2024. See Appendix for full map catalogue.




**Map:** Russia & Baltic area, August 2024. See Appendix for full map catalogue.

# Spoofing detailed by region

As of August 2024, the following are the **major spoofing areas** worldwide. Locations can change without notice, but all these regions have had steady spoofing impact throughout 2024.

## 1. Eastern Mediterranean Sea area

**Nicosia FIR - Cyprus**. Currently the highest spoofed FIR worldwide. Spoofing related to Israel conflict. All routes, entire FIR. Includes approaches to LCLK/Larnaca and on-ground spoofing. Spoofed-to position was mostly OLBA/Beirut; as of August 24, 2024, that changed to mostly OJAI/Amman.

**Beirut FIR – Lebanon**. Entire FIR. Traffic into OLBA/Beirut airport is regularly spoofed, and on-ground spoofing is common. IRS alignment issues noted. Go-arounds common due to system issues on approach.

**Tel Aviv FIR – Israel**. Entire FIR at risk of spoofing. LLBG arrivals/departures affected, caution wayward SID tracking and proximity to danger and military areas. On-ground spoofing possible.

**Cairo FIR – Egypt**. Especially over Sinai peninsula, north-eastern portion of the FIR, and at Cairo airport. Spoofed-to positions include Beirut, Tel Aviv, Cairo, and Amman. On-ground spoofing possible at HECA/Cairo. Airways L550, L560 most affected, also A16, and any traffic within 200nm of CVO (Cairo) VOR.

**Jeddah FIR – Saudi Arabia**. Traffic routing to/from Egypt is usually spoofed close to Cairo FIR boundary. Airway/position. Spoofed-to positions include Beirut, Tel Aviv, Cairo, and Amman. Airways L550, L560, UB411 (which carry high levels of east-west traffic) most affected.

**Amman FIR – Jordan**. Traffic landing at Jordanian airports (OJAM/Amman Marka, OJAI/Queen Alia, OJAQ/Aqaba) regularly spoofed, causing issues with RNP approaches. Entire FIR carries spoofing risk.

## 2. Black Sea area

**Ankara/Istanbul FIRs - Turkey**. High levels of spoofing on the northern Turkish coastline, and the western Black Sea area, near Istanbul. Airways UM859, UN743, UL746 most affected. Spoofing here is more commonly preceded by jamming. Spoofed-to position mostly Simferopol airport (Crimea). A second spoofed-to position near Krasnodar identified in June 2024. Region active since March 2024.

**Sofia FIR - Bulgaria.** Spoofing active in overwater areas in the east of the Sofia FIR, and over land close to the Black Sea coastline, in the area of Burgas and Varna. Affects mostly transit traffic EU-Asia. Spoofed-to position mostly Simferopol.

**Bucharest FIR – Romania**. South-east quadrant of the FIR sees 90% of the spoofing, in the area between Brasov, Bucharest and Constanta. Affects mostly transit traffic EU-Asia. Spoofed-to position mostly Simferopol.

## 3. Russia & Baltic region

**Samara & Moscow FIRs - Russia**. Hotspots are Nizhny Novgorod and Samara, with high levels of spoofing in these areas. Spoofed-to locations show Moscow and Yaroslavl.

**Tallinn, Riga and Vilnius FIRs – Estonia, Latvia, Lithuania.** Spoofing most noted in the eastern parts of Riga FIR (Latvia) and Vilnius FIR (Lithuania). Airway M864 is the most affected. Spoofed-to location typically Smolensk.

**Helsinki FIR – Finland**. Spoofing is most common on the Helsinki/Tallinn FIR boundary, mostly used by Russian aircraft transiting to Kaliningrad, but also noted around EFLA/Lahti and EFHK/Helsinki. Spoofed-to location is Smolensk.

## 4. India/Pakistan border

**Lahore & Delhi FIRs – Pakistan & India**. Daily spoofing has been occurring here since May 2024. Areas north-west of New Delhi, and in the area of Lahore, are the most affected. Spoofed-to locations generally along the line of the border.

## Previous spoofing locations

**Iraq, Iran** (Baghdad and Tehran FIRs). Initially a major location, now minor. In the first wave of GPS Spoofing incidents, 80% were occurring in an area between ORBI/Baghdad airport and the northern ORBB/Baghdad FIR boundary, and close to the Iranian border (OIIX/Tehran FIR). Sporadic/occasional spoofing seen again August 2024.

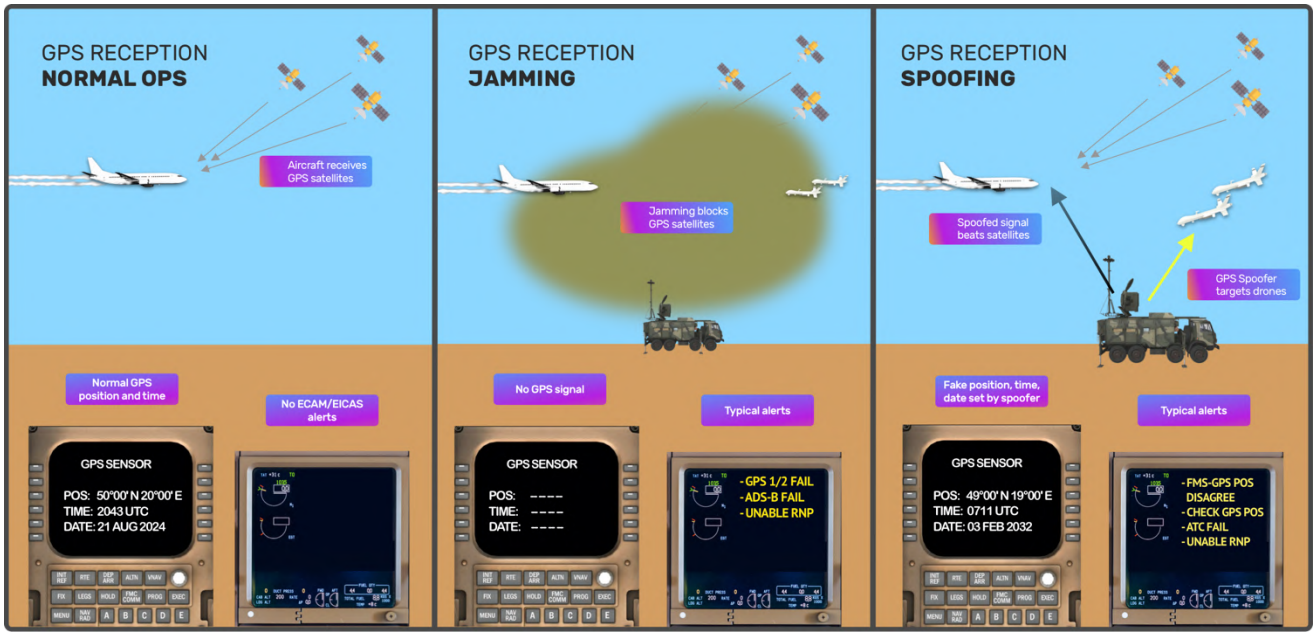
**North/South Korea** (Pyongyang and Incheon FIRs). A period of GPS Spoofing was recorded in June 2024. The majority occurred near the North/South Korean border. A small number of spoofing incidents seen in the oceanic portion of the FIR.

**China**. A number of reports, and correlated data, showed spoofing near Beijing airport in May 2024. No recent reports.

# How GPS Spoofing works

In **normal operation**, the aircraft GPS Receiver receives Position, Navigation, and Timing information from a constellation of satellites.

In the **spoofing situations** now commonly encountered, a ground-based spoofing platform broadcasts **fake signals**, which are interpreted as valid by the aircraft GPS receiver. False position and time information is then fed from the GPS receiver to other aircraft systems.




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

During **GPS Jamming**, a radio transmitter, generally ground-based, transmits noise or interference on the GPS frequency band(s). As a result, the aircraft GPS receiver loses the satellite signal.

During **GPS spoofing**, another ground-based transmitter (or group of transmitters) begins to send a fake GPS signal, causing GPS receivers to calculate incorrect position, time, and altitude. Since satellite signals are very low power, the spoofed GPS signal overpowers these quite easily. The aircraft GPS receiver now takes the fake signal as true, and begins to share the new false position with aircraft systems.

For most spoofing affecting civil aviation at present, these jamming and spoofing transmitters are high-grade military equipment, either portable on a vehicle, or moveable units installed at fixed locations. An example is the Russian spoofing platform on an oil rig in the Black Sea, destroyed by Ukraine in early August 2024 (see "Equipment types" later in this report for more detail).

Although these counterfeit signals resemble the genuine signal, they may differ in various ways to fool the GPS receiver:

- Code (and carrier) phase drift
- Altered navigation data: incorrect orbit biases that alter the position completely, or setting some or all satellites to unhealthy.
- Incorrect timestamps broadcast from each satellite. Since a GNSS receiver calculates a spacetime coordinate and a velocity, a spoofer can force a receiver to calculate the wrong position, altitude, speed, time, and date.

An effective method of spoofing receivers with no inherent spoofer protections involves broadcasting a jamming signal that overpowers the existing real signals coming from space ("raising the signal noise floor") and then broadcasting "louder" (but not too loud) spoofing signals on top of this. This causes the true signals from space to get "buried" and the only signals that the receiver will be able to find and decode are the spoofer signals. The receiver will still calculate a signal to noise ratio that is sensible, even though the actual signal powers are much higher than the real ones from space.

In a "targeted" or "synchronous" spoofing attack, a spoofer undergoes a complicated procedure of "capturing" a specific, single target receiver directly by overlaying their counterfeit signals perfectly with the receiver's copies from space, gradually raising the power to "steal" the receiver from the true signals, and then adjust the signal accordingly to drag the receiver off from the true signals. The spoofer needs to know the receiver's position and velocity accurately, so the attack is most easily carried out on static receivers. The nature of the spoofing being encountered by civil aviation is however not currently this targeted kind.


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.

# Terminology: GNSS vs GPS

Though technically inaccurate, the terms GPS and GNSS are used interchangeably in the aviation industry. GNSS (Global Navigation Satellite System) is an umbrella term covering any satellite constellation that provides positioning, navigation, and timing (PNT) services, and includes Satellite Based Augmentation Systems (SBAS), such as the US Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay System (EGNOS).

The four main GNSS systems in use today are GPS (USA), Galileo (Europe), Beidou (China) and GLONASS (Russia). India (IRNS) and Japan (QZSS) also operate regional GNSS systems.

**GPS (Global Positioning System) is the predominant GNSS system**. Most aircraft systems documentation refers to "GPS" rather than "GNSS", and flight crew use "GPS" as standard terminology.

**We therefore use the term "GPS" in this report.**

# Spoofing location terminology

**Spoofing Location**
Where an aircraft can expect to experience GPS Spoofing

**Spoofed-to position**
The false GPS coordinates received by the aircraft GPS receiver.

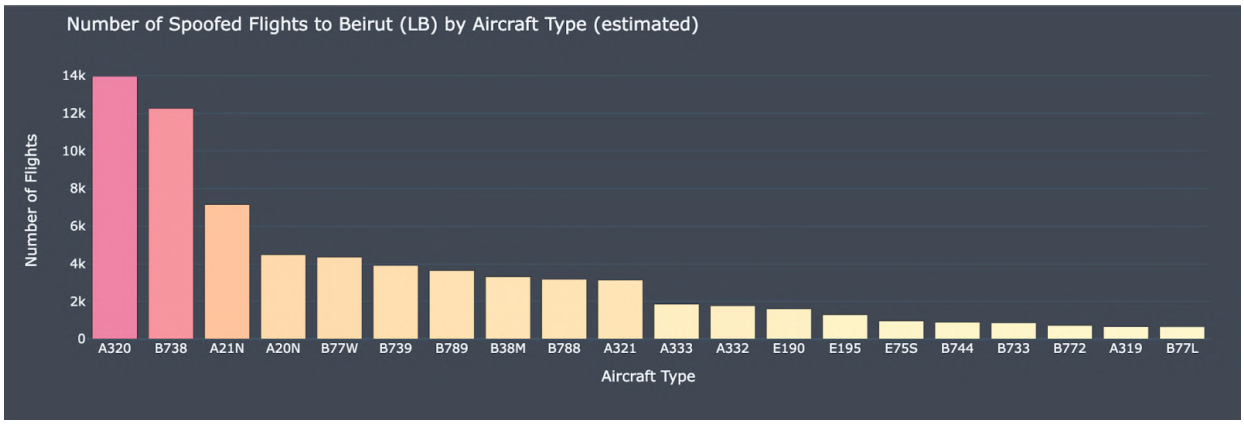
**Spoofing Transmission Source**
Where the Spoofing equipment is located. This may be a single transmitter or a network of transmitters. It's important to note the location of the spoofing transmission source is usually **not** the same as the spoofed-to position.

# Aircraft Types affected

An analysis of the different aircraft types affected by GPS spoofing reveals that all GPS-equipped airframes are vulnerable to this threat.

The figures below show the top fifteen aircraft types affected during the period January - July 2024 in two example areas: the Black Sea and the Middle East.

In this data, the number of flights affected by type is more representative of the traffic types in the regions – the Eastern Mediterranean has far more short- and medium- haul traffic than the Black Sea region.

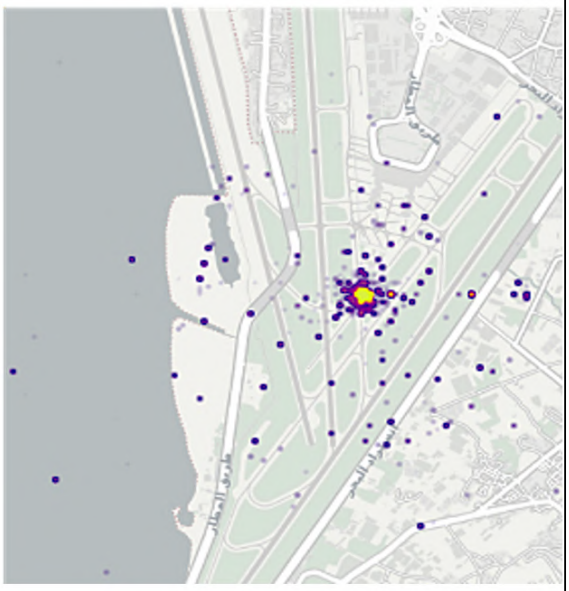
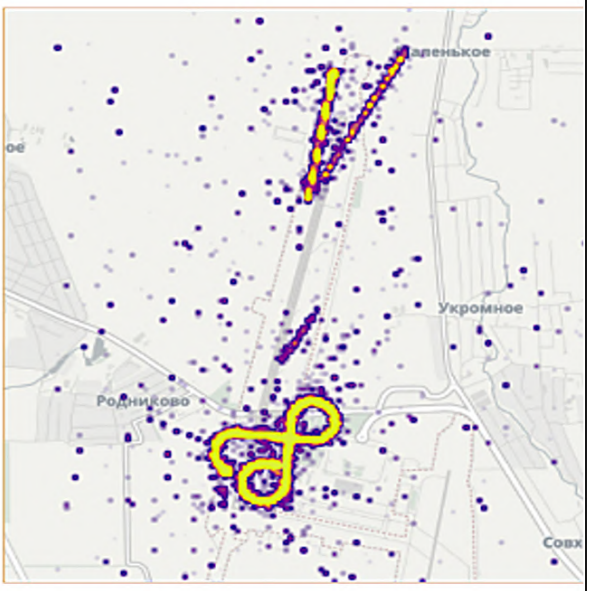


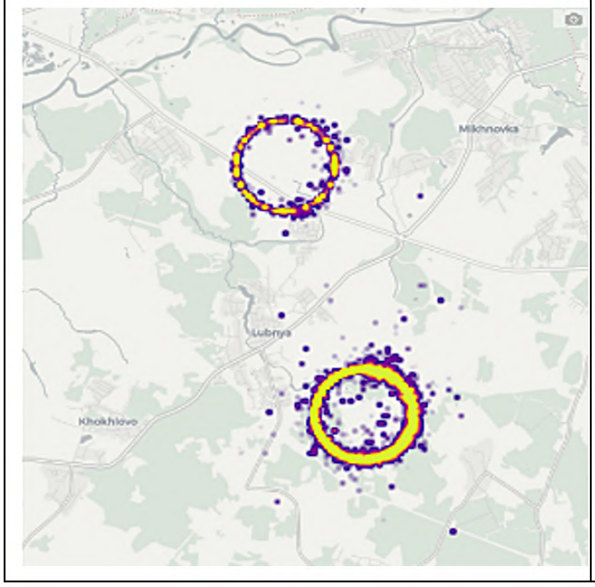

Data source: ZHAW/SkAI.

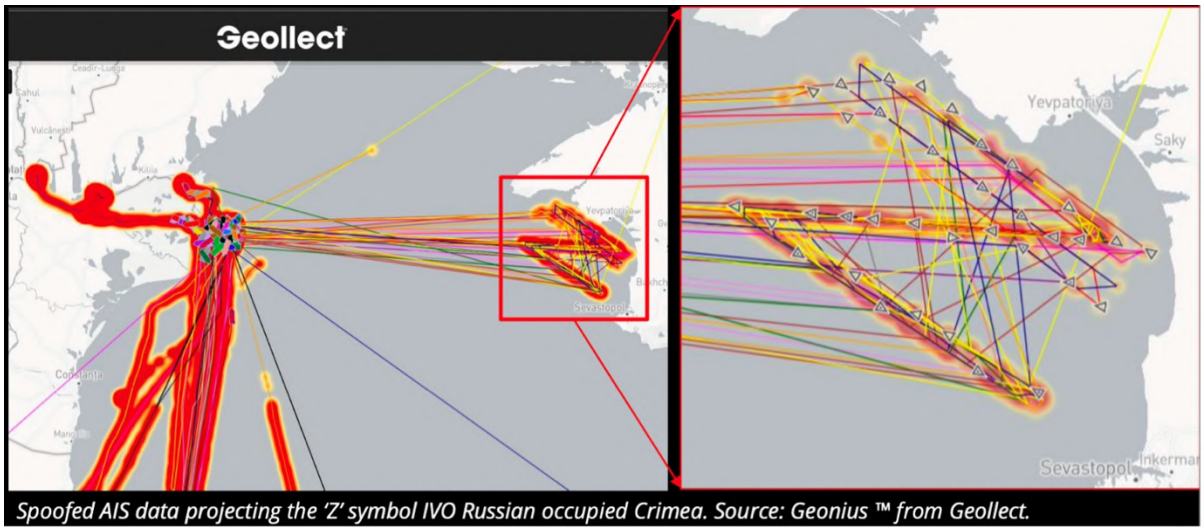

Data source: ZHAW/SkAI.

# Spoofing Patterns

The falsified GPS positions created by spoofers aren't always the same. In some cases they are fixed in one place, but in other examples seen they move in circles, form complex patterns, or even mimic realistic paths.

| Static Location at Beirut Airport: | Complex patterns at Simferopol |
|---|---|
|  |  |

| Circular Spoofing near Smolensk: | Along a realistic path in Ukraine: |
|---|---|
|  |  |




*Spoofed AIS data projecting the 'Z' symbol IVO Russian occupied Crimea. Source: Geonius ™ from Geollect.*

# Typical GPS Spoofing Equipment

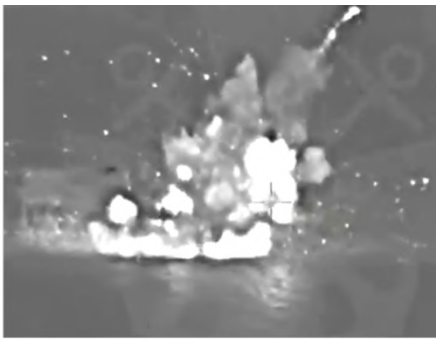
As noted above, almost all spoofing currently affecting civil aviation is being carried out by large-scale military Electronic Warfare equipment, by multiple countries. Examples of the this type equipment are below.

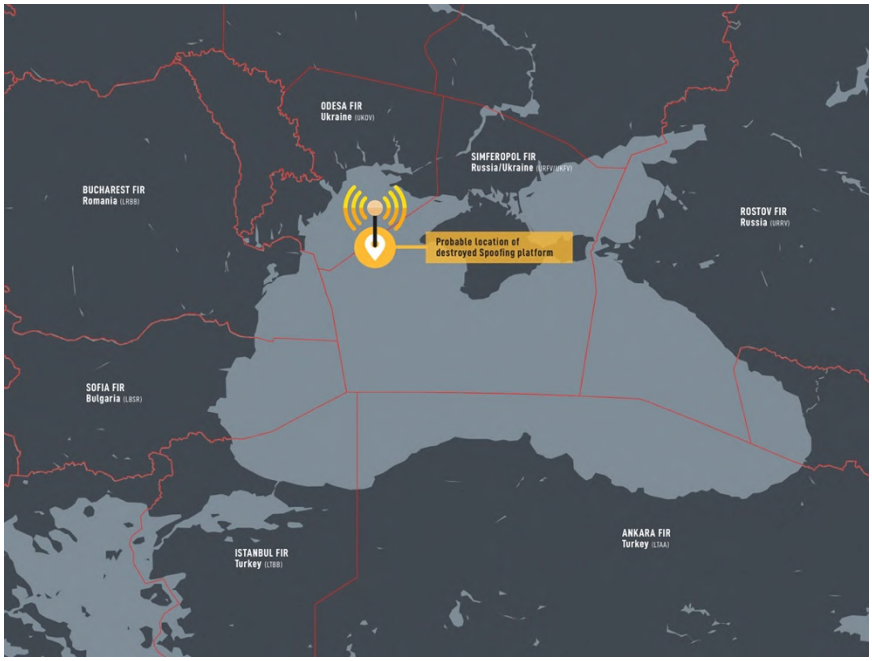
*The R-330Zh Zhitel is a mobile truck-mounted electronic warfare (EW) station*

*The Krasukha is a mobile, ground-based, electronic warfare (EW) system*

## Oil Rig GPS Spoofing Platforms

In August 2024, a disused oil rig being used by Russian forces for GPS Spoofing was destroyed by Ukraine. As a result, spoofing levels in the Black Sea area reduced significantly, confirmed by data from SkAI and Spirent. The Ukrainian Navy said "[Russian forces] used this location for GPS spoofing to endanger civilian navigation. We cannot allow this". The target of the spoofing was on maritime vessels, but civilian aircraft receive the same spoofed signals.



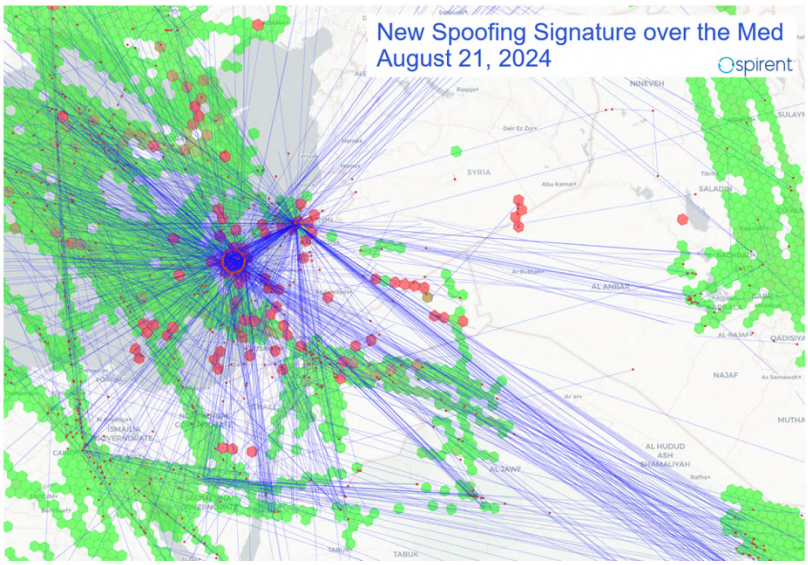


# Changes in Spoofing Locations and Patterns

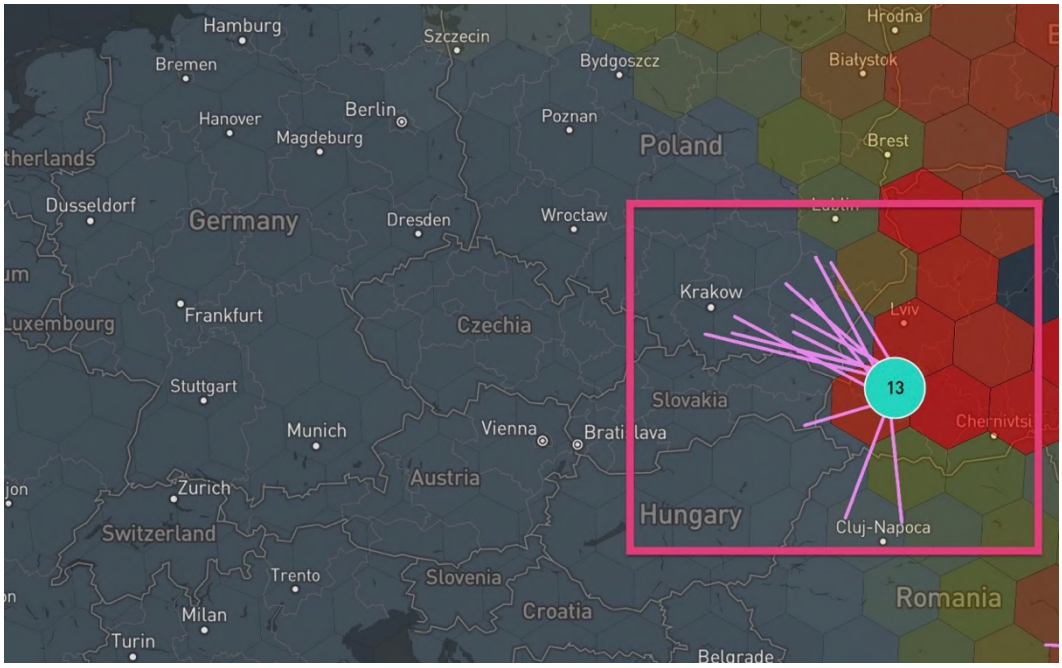
There is constant evolution in GPS Spoofing locations and patterns, with significant changes as often as weekly or even daily. This highlights the need for operators and crews to have access to a very current spoofing location map. Some examples of changes are below.

### Changed spoofing pattern in the eastern Mediterranean, August 2024

- Spoofing is always changing
- New "spoofed to" circle over the Mediterranean Sea
- Slightly larger "alert area"
- Most flights impacted by:
  1. New circle spoof
  2. Scattered location over Beirut
  3. Scattered location over Israel
- GPS integrity varies by aircraft type and hence impact to crews & systems
- Some aircraft continue to have GPS issues after exiting the spoofed area (not shown)
- Detected in real-time service & replicated in test equipment




### New Spoofing location in western Ukraine, August 2024



# Further Technical Information

## Spoofing Tactics

- A spoofing technique employed by one "state actor" is to jam the secure GPS L2 frequency (1227.60 MHz), whose Precise Code (P-Code) is used by military systems to provide increased PNT performance, to force the use of the Civil Access (C/A) code on the L1 (1575.42 MHz) frequency. The state actor then spoofs the unsecured L1 signal. **It makes the spoofing easier**, because they only need to spoof one set of signals. The second civil frequency L5 signal (1176.45 MHz), which has not yet been incorporated in avionics GPS receivers and is not fully supported by the constellation, is stronger than L1 and will require higher powered jammers however, these are also emerging in some theatres of operation.

- At the moment, the dominant factors in a spoofer selecting constellations, frequencies, and codes to broadcast will be power budget and the most commonly used signals. Transmitting maximum power on only one frequency gives much greater jamming and spoofing range than transmitting that same maximum power over many more frequencies and signals. However, as receivers move to use more frequencies and signals, it will not be difficult for the spoofers to adjust. So, using more than one GNSS constellation and using more than one frequency (e.g., GPS L1 and L5) may provide a very short term protection in some areas, but it **is not a long term solution** to the problem beyond the time taken for the spoofers to change some settings in their menus on their spoofing devices.

## Code phase

The time delay for a GPS satellite signal to travel from the satellite to the receiver provides the measure of the distance between the satellite and the receiver. However, this distance measurement is impacted by delays that occur as the signal passes through the ionosphere. Augmentation systems, such as WAAS and EGNOS provide data to allow these errors in distance measurements to be removed. The code phase of the received signal is a measure for this distance and refers to what section of a given satellite's coded broadcast is arriving at a particular moment in time. The code phase is estimated by matching the satellite's unique Pseudo Random Number (PRN) code with a local copy of this code. If there is a match, then the receiver has detected the signal (see acquisition above). These codes are 1 millisecond long for GPS C/A and 4 milliseconds long for Galileo E1, and due to the speed of light these codes effectively each span a distance of 300 km long and 1200 km long respectively from end to end when broadcast. By measuring the code phase accurately to a few nanoseconds, the receiver can calculate the distance to the satellite to an accuracy of a few meters. The carrier phase can also be measured to determine the distance between satellite and receiver to an accuracy of centimeters.

## Navigation data

The navigation data contain various parameters that are used during the operation of the receiver such as satellite orbital parameters and clock corrections. Also, the navigation data provide an indication of the GPS satellites' health. If the spoofer broadcasts incorrect navigation data (which is generally the case), then the GNSS receiver may continue to calculate incorrect results even after it leaves the spoofing area and receives the true ranging signals again. This will continue to be the case until the receiver is manually reset or the navigation data "expires" and is refreshed automatically (which may never happen if the spoofer broadcasts its data such that the spoofed navigation data expiration date has been set to some time well in the future).

## Doppler shift

GPS satellites orbit approximately 20,200 km above the Earth in what is called Medium Earth Orbit (MEO) and travel with great speed relative to receivers. This speed relative to the receiver results in a Doppler shift in the received signal compared to a situation where both the transmitter and the receiver are static. The Doppler shift measurements are used in both the position and velocity calculations for the receiver. Monitoring abnormal Doppler measurements compared to other sources of velocity on the aircraft provides receiver manufacturers with a valuable indicator of potential spoofing attacks.

## RAIM

GPS receivers have Receiver Autonomous Integrity Monitoring (RAIM) algorithms to detect and mitigate erroneous GPS signals. These algorithms offer some protection against errors from a faulty satellite broadcast. For example, RAIM detects spoofing where the receiver tracks both real and fake satellite signals that cause inconsistent measurement data if only one or a very small number of signals are affected by spoofing and the vast majority are not. The RAIM Horizontal Integrity Limit (HIL) must be valid before the GPS output is used by airplane systems.

Traditional RAIM algorithms protect against a single faulty satellite by trying all "leave one out" PVT solution calculations. If one position fix is clearly different from the rest with much lower residual errors on each signal going into that fix it reveals the presence of a single faulty satellite. The computational load increase of moving from 1 faulty satellite to N faulty satellites is exponential. **RAIM was never designed to protect against spoofing and is not able to detect a case where all the signals are spoofed and would thus all deliver consistent information**.

## Concern of corrupted GPS receiver appearing normal

Due to the way GPS receivers are designed, the only way to ensure that a GPS receiver will be trustable after any exposure at all to a spoofing attack is to fully reset the internal states of the receiver, by power cycling it, or by sending a "cold restart" command in software. There are even examples of some receivers that have been so disrupted that a full factory reset by returning the device to the manufacturer has been required.

This is true even if the receiver "**appears to have recovered**" after leaving a spoofing region. It is in fact still possible for the receiver to output false information later on in the flight, even hours later. For the interested reader, a full explanation of this is given here.

The orbital data for each satellite is continually broadcast by each satellite, and the receiver downloads the orbital data from each satellite regularly. This data is called the *ephemeris*. It takes about 20 -30 seconds to download it and each satellite only broadcasts their own. The ephemeris contains within it a timestamp which acts as an "expiry time" for that dataset. If the current time is too long after the expiry time the receiver will typically refuse to use that orbital data and will wait for fresh ephemeris to be downloaded.

If you have incorrect ephemeris data (e.g., a corrupted download, or because of a spoofing attack), you can't calculate the correct distance to the satellite when receiving its timing data. The following worst-case scenario addresses the case where a receiver continues to output corrupted measurements many hours after leaving a spoofing area.

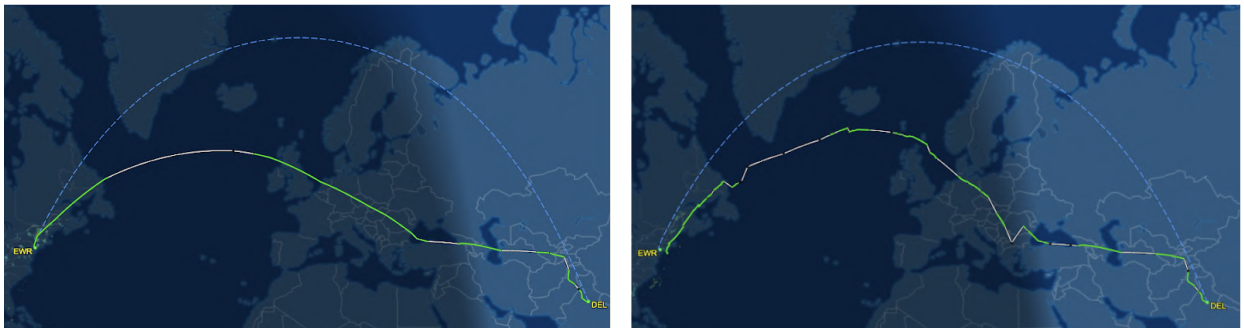
In this scenario, consider a receiver that is initially working correctly and is tracking the GPS satellites numbered 1, 2, 3, ....8, 9, 10 that are currently above the horizon. The other satellites are currently below the horizon. The receiver now flies into a jamming and spoofing zone. The receiver loses the lock of the satellites in the sky. The spoofer is broadcasting satellites 13, 14, 15, ..., 19, 20 and so the receiver locks onto and downloads all of those ephemerides (from the spoofer's signals not from the real satellites). The spoofer is also transmitting the time a few hours into the future (we regularly see spoofed times and dates set to the future in the current interference regions). The receiver is then spoofed and reports incorrect positions, velocities, and times. The pilot ignores the data and flies through the spoofing region. The spoofed signals for satellites 13 to 20 fade away, as does the jamming signal, and the receiver picks up the signals from the real sky again, i.e. satellites 1,2, 3....to 10. The position fixes and time all now look correct, and it may reasonably be assumed that the receiver has recovered. However this is not the case at all, as will now be explained.

As the aircraft continues its planned flight and an hour or more passes, the satellites visible in the sky start to change. Some of the satellites in the set 1, 2, 3...10 pass over the horizon and some of the real satellites from the spoofed set 14 to 20 are now rising in the sky. The receiver locks onto them and decodes the timing data and ephemerides from the real satellites. However the corresponding time of applicability for the spoofed data has remained in the receiver's memory, and the key time stamp is still an hour later in time than the one being broadcast by the real satellites in the sky. As a result, the critical software code inside the receiver that checks these timestamps does not trigger the replacement of the spoofed orbital data with the real data. This will only occur at some point in the future when enough time has passed for the "expiry time" for the spoofed ephemeris data to finally be at some point in the past, rather than still being in the future. So, now the problems begin:

The receiver now tries to use the real satellite measurements with the incorrect spoofed orbital data still stored in its memory. The result is that there are nonsensical calculations and large discrepancies among the satellite measurements. Using an approach called "Receiver Autonomous Integrity Monitoring (RAIM)" the receiver attempts to detect and ignore a single "broken" satellite. The navigation system's Kalman Filter also provides another layer of protection against a small number of erroneous satellite measurements. However, as time passes further and satellites keep rising and setting, eventually very few usable satellites are visible and the majority of the authentic GPS signals are coming from the set 14 to 20, with incorrect orbital data. By now the receiver is outputting unusable and erroneous data and it is likely that its performance will have further degraded as the "good" satellites disappear one-by-one below the horizon. Although the time will be correct, the positioning has gotten worse and worse over time. The best case scenario now is for the receiver to cold restart itself, but most will not do this. They will instead do a "warm restart", which means reacquiring the satellites and restarting the Kalman Filter, but critically not wiping all of the orbital data from memory.

While this scenario might not occur after every spoofing event, it is a plausible scenario and evidence exists that such scenarios may indeed be playing out. The image below shows UAL83's 22 May 2024 and 1 August 2024 flight from Delhi, India (VIDP) to Newark, USA (KEWR). While the May flight path is as expected, the August flight exhibits a highly unusual tracking solution, which neither conforms to the expected flight path nor looks like a coasting inertial reference system (which would show a smooth divergence over time without jagged resets and jumps). Nor does it look like a functioning GNSS receiver. The behavior that it does exhibit can be explained by a GPS receiver that keeps resetting its navigation Kalman Filter, but is forced to keep calculating fixes using a mixture of valid and invalid measurements.

Different receivers may have different logic and thresholds for how and when to refresh the orbital data for all satellites, and so the scenario above should be discussed with GPS receiver providers to understand under exactly what scenarios a receiver would and would not replace the current orbital data with new data being decoded from the satellites.




These figures show UAL83 DEL-EWR flights on 22 May 2024 (left) and 1 August 2024 (right). The journey on the left seems to be an example of the expected route for this journey. The journey on the right exhibits significant and sustained disruption to the tracking performance for the entire flight, following an exposure to GPS spoofing early on in the flight.

**Figure 3** GPS Spoofing Location Map – Worldwide

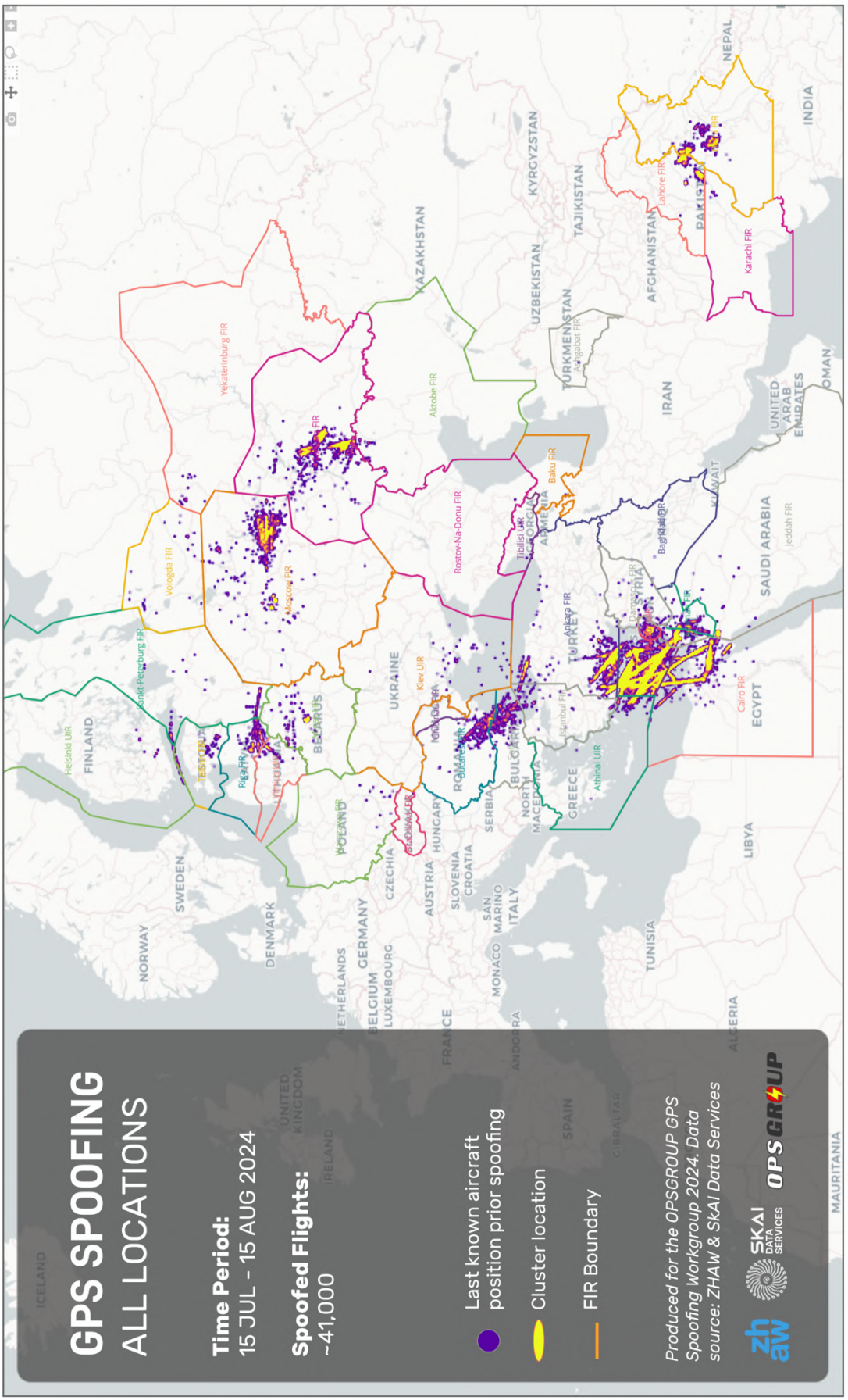


**Figure 4** GPS Spoofing Location Map – Eastern Mediterranean

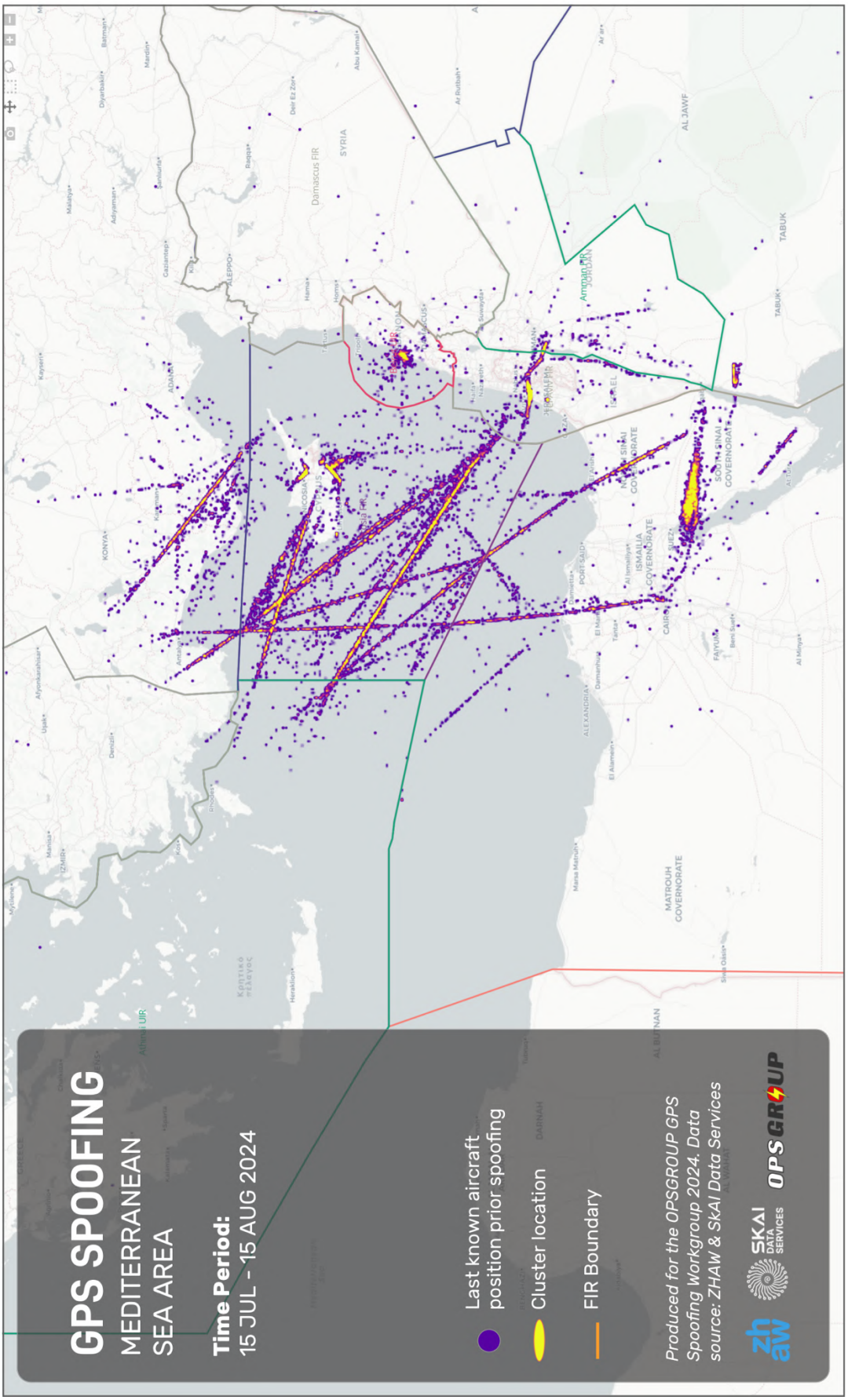


**Figure 5** GPS Spoofing Location Map – Black Sea

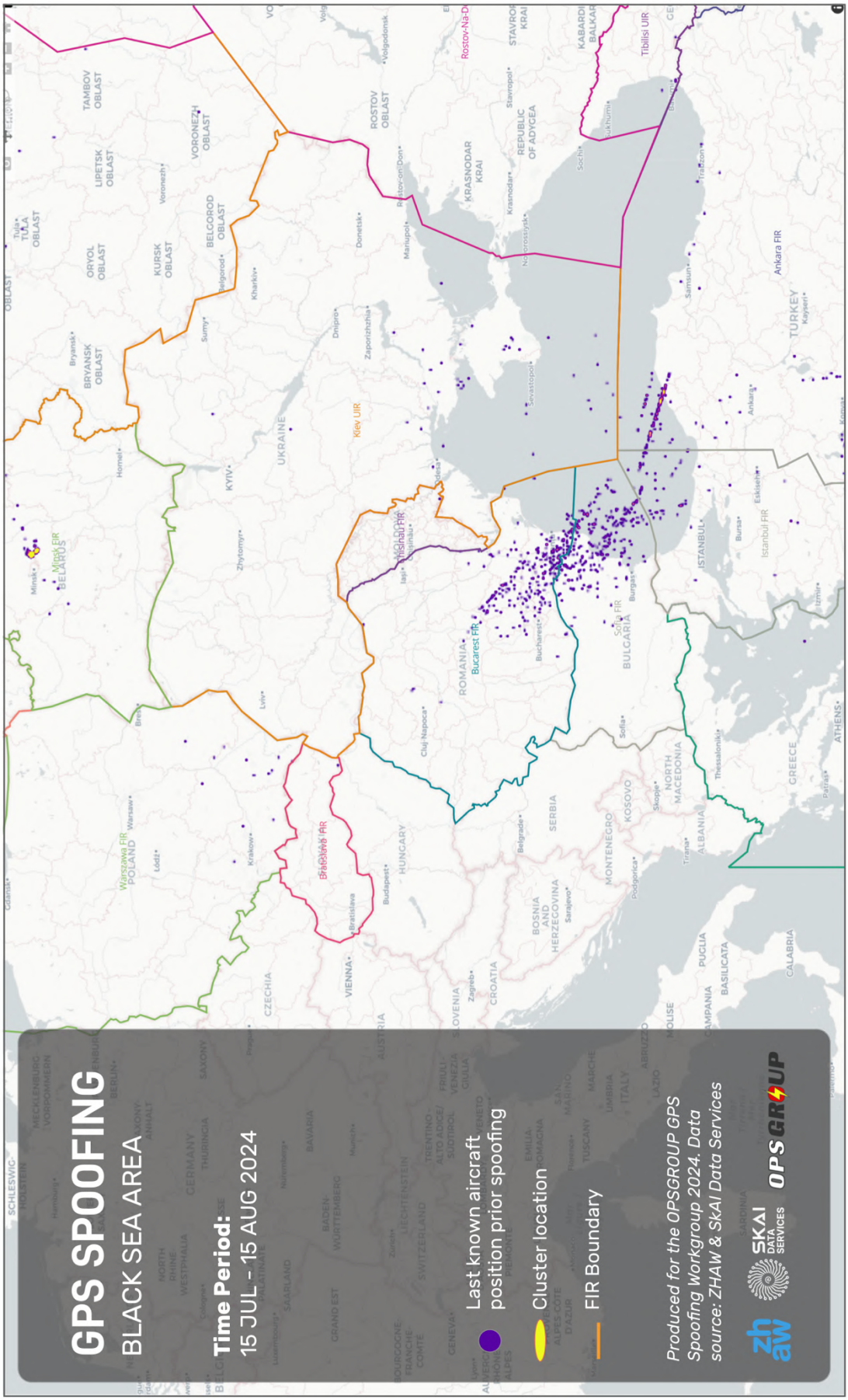


**Figure 6** GPS Spoofing Location Map – Russia & Baltic Area

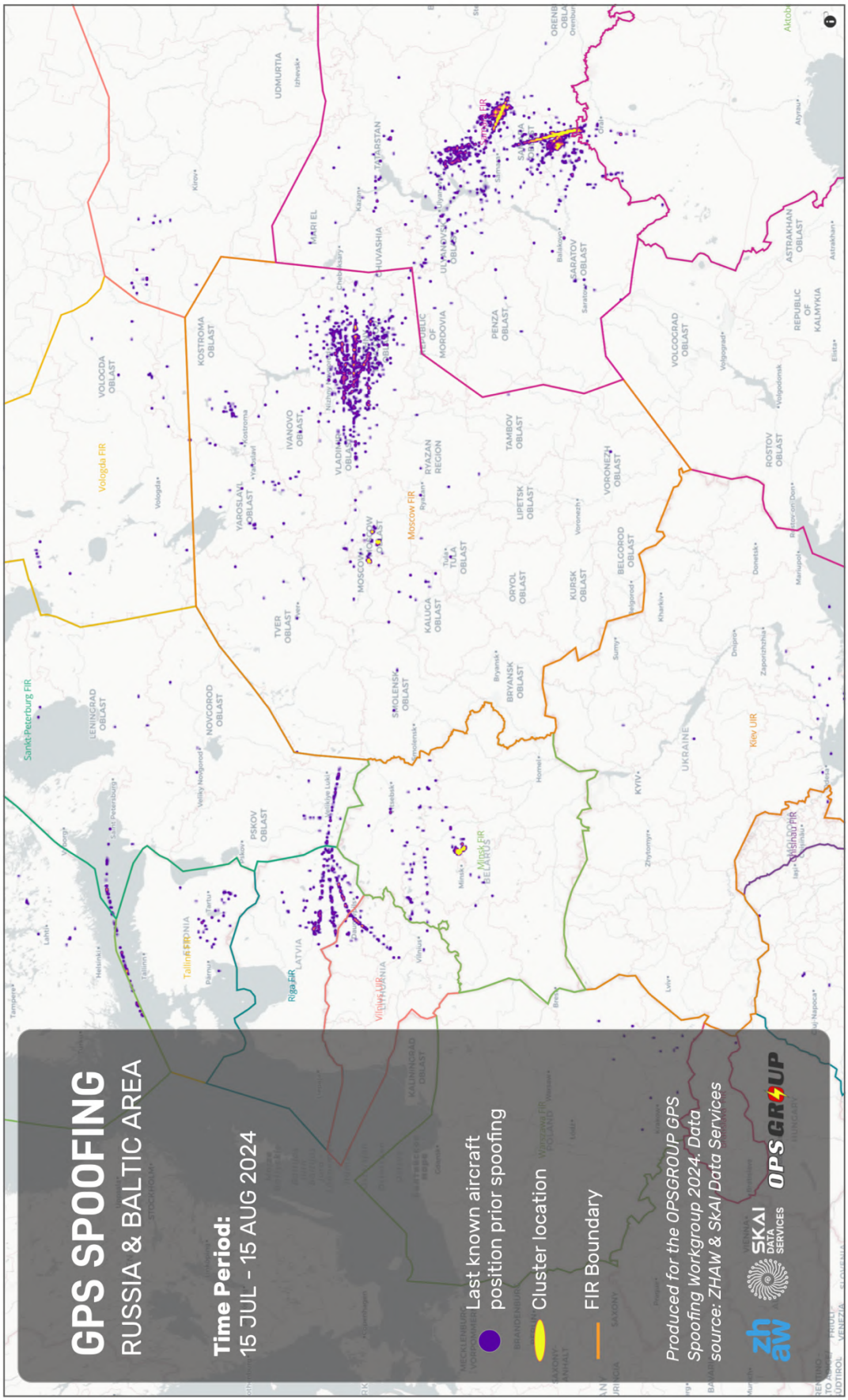


**Figure 7** GPS Spoofing Location Map – India/Pakistan