Monitoring and Detection of GNSS Interference Using the Swedish CORS Network SWEPOS

Kibrom Ebuy Abraha, Tobias Nilsson

EUREF Symposium 2023
May 23-26, 2023, Gothenburg, Sweden

LANTMÄTERIET

Outline

- GNSS vulnerability – Taxonomy
- GNSS interference threats
- GNSS interference monitoring at SWEPOS

GNSS Vulnerability

GNSS Cybersecurity

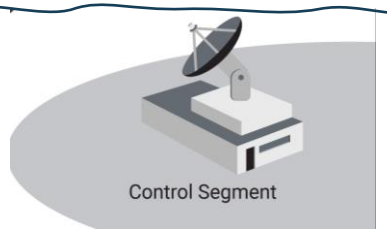
Space Segment

- Space weather
- Satellite attacks

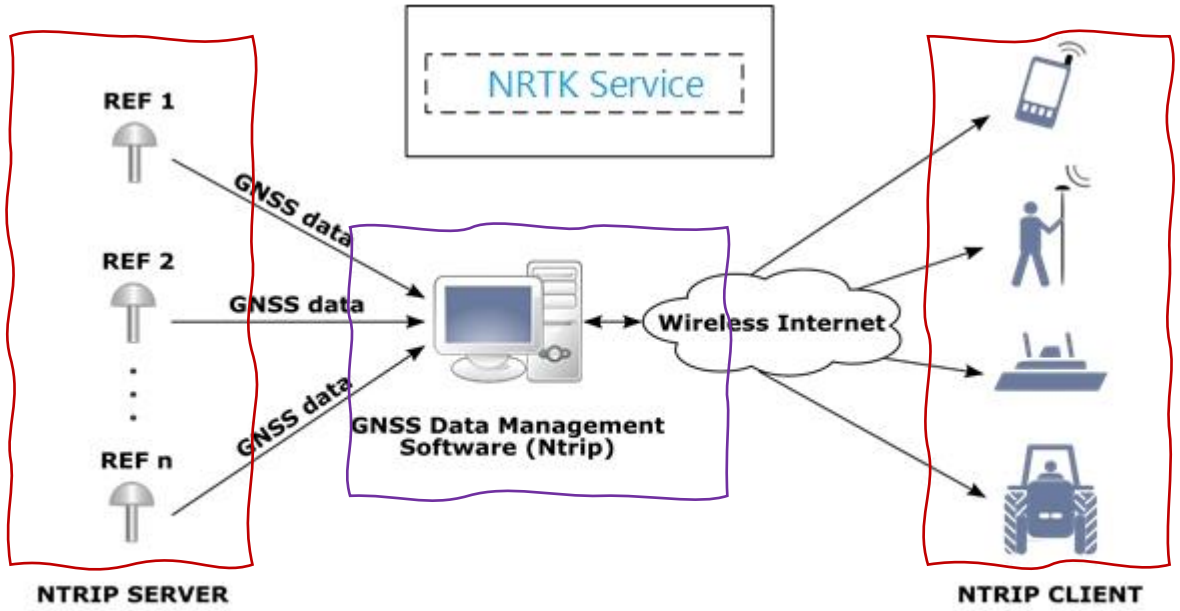
When will Russia attack GPS? Interview with former CIA analyst George Beebe

February 24, 2022 · By Dana Goward · Est. reading time: 3:30

- System hack



User Segment



GNSS Interferences

- Jamming
- Spoofing
- Meaconing

- System hack

GNSS interferen s

- GNSS signals
  can easily b
- Wider fr
- Increa onal
  - al
  - cipat
  - ono
    R
    - anten
  - – Dis
  - ing –

More Russian GPS jamming than ever across border to Norway

Four passenger aircraft have over the last few days lost GPS signals when flying in Norway's northeastern region. Since Russia's invasion of Ukraine, jamming has been registered more than 20 days.

This article is more than 1 year old

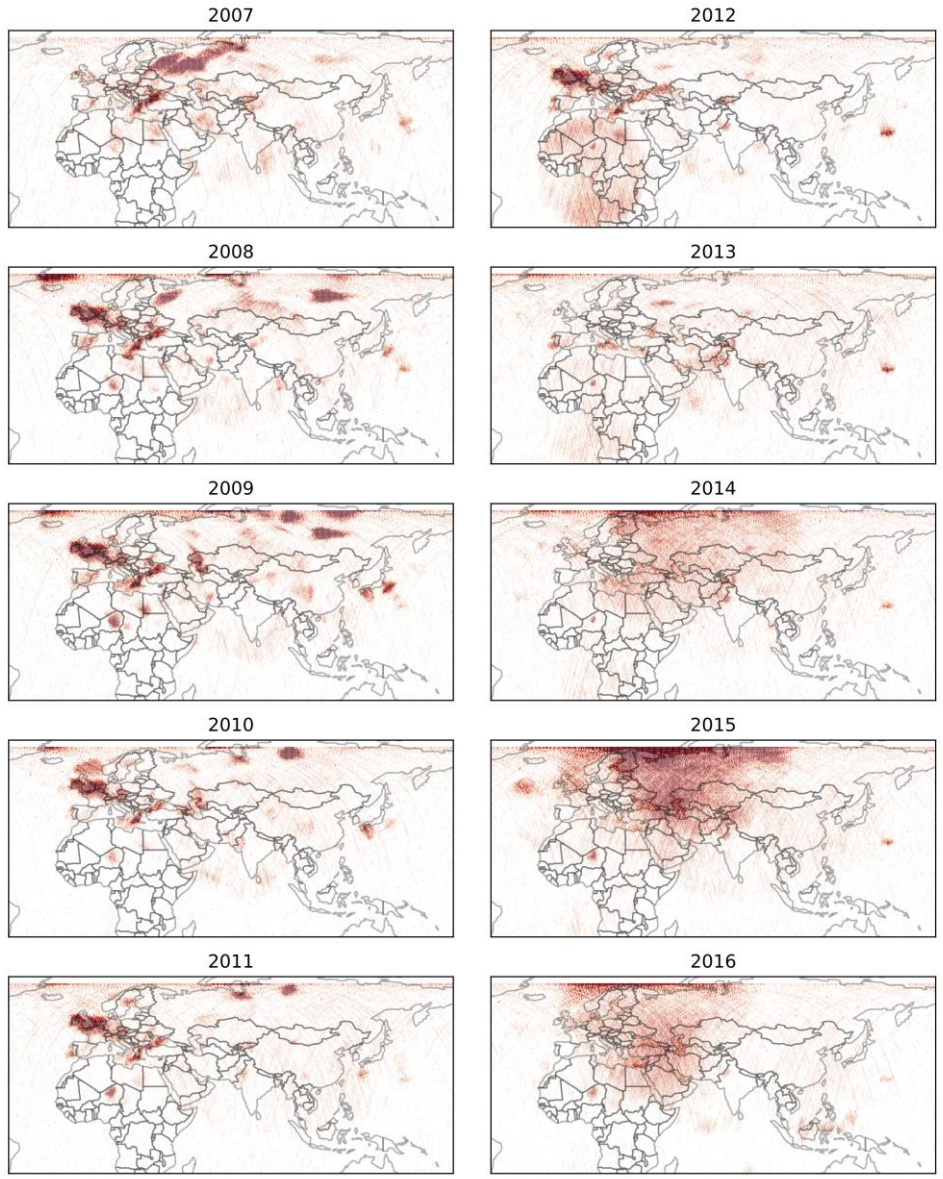
Finland reports GPS disturbances in aircraft flying over Russia's Kaliningrad

Australian aircraft's GPS receiver jammed by alleged Chinese warships

March 23, 2023 - By Maddie Saines

https://safetyfirst.airbus.com/gnss-interference/

- Temporal variations of RFI over Europe, Asia, Africa
- Russia-Ukraine conflict effect visible in 2014-2016
  - Roberts M et al 2021



SWEPOS GNSS Signal disturbance monitoring and detection - Goals

Monitor

- Monitoring of anomalous events
- Using GNSS geodetic infrastructure – SWEPOS (not external monitoring system)
- Characterizing GNSS signals
- Monitoring signal strength
- Consistency check

Detect

- Detect anomalous events
- Classify anomalous events
- Multipath? Equipment failure? RFI?

Respond

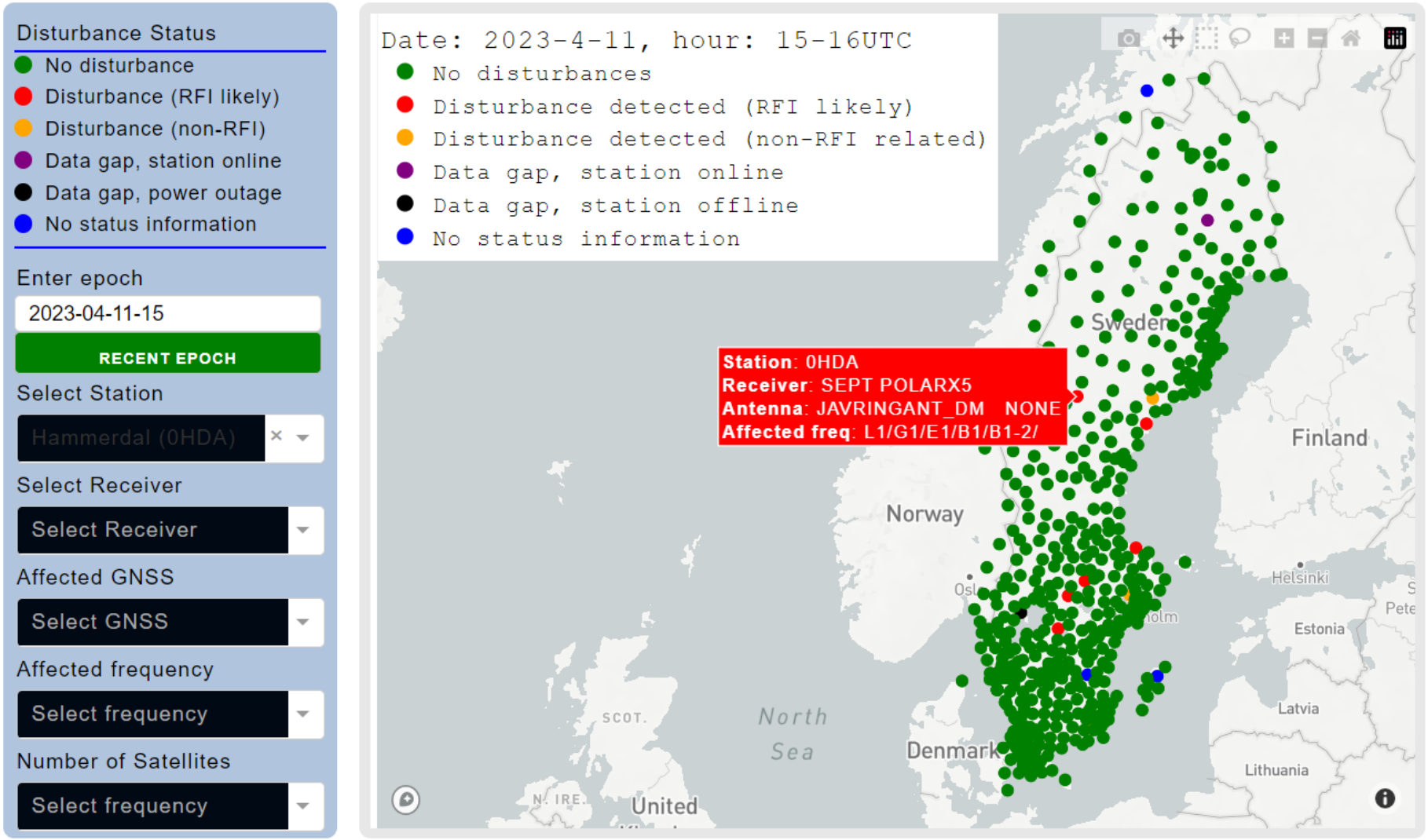
- Contain the event
- Geolocate the source
- Assess the impact and continuity of the event
- Mitigate it
  - Receivers, softwares
- Inform users

Unmitigated interference

- Flag off the station
- Move the station
- GNSS dependent Infrastructures should have a clear plan of recovering their system in the event of large scale attacks and have other alternatives.

SWEPOS® GNSS interference Monitoring

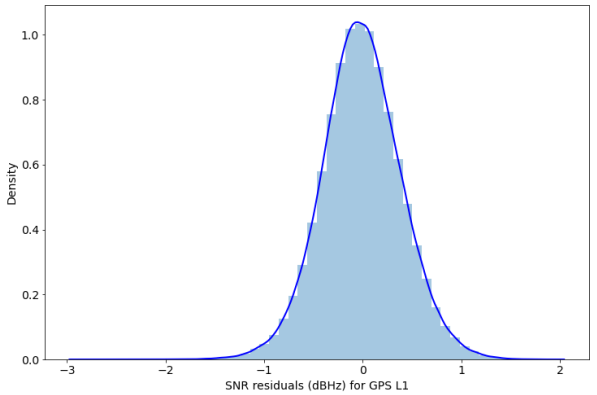
- Monitors all Swepos stations + third party stations = ~544 stations

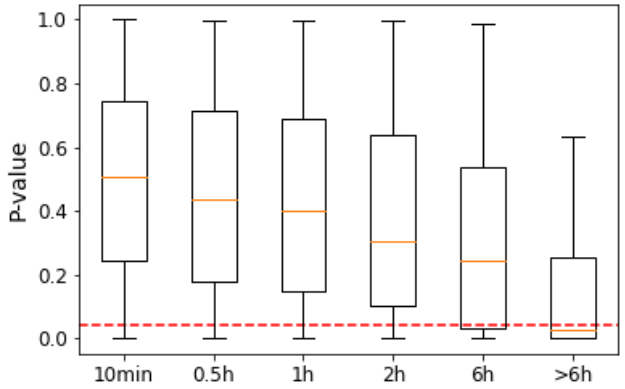


SNR residuals characteristics

- Model SNR for each satellite (it takes receiver, elevation, azimuth and other dependent effects into account)
- Get SNR residuals (model – data) for each satellite

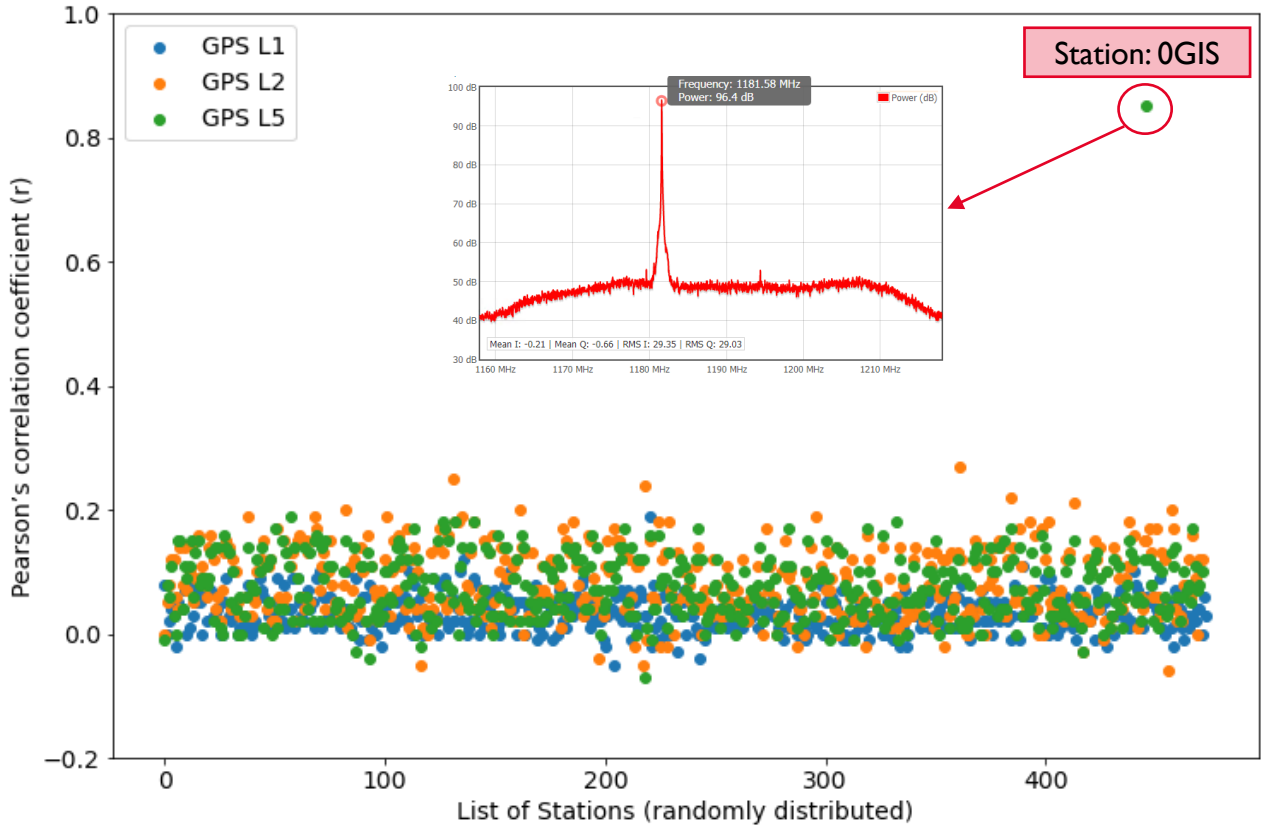
- SNR changes slowly unless interference is present
- Over a short period of time SNR can be treated as a stationary process
- Normally distributed
  - Shapiro-Wilk normality test of SNR residuals
  - Null hypothesis – residuals are normally distributed
  - Null-hypothesis is rejected for p-value < 0.05 (red-dotted line)
  - SNR residuals normally distributed over shorter periods
  - Over longer periods (longer than 6 hours), p-values fall below 0.05 for most of the stations





SNR residuals characteristics

- Cross correlation of SNR residuals among simultaneously tracked satellites.

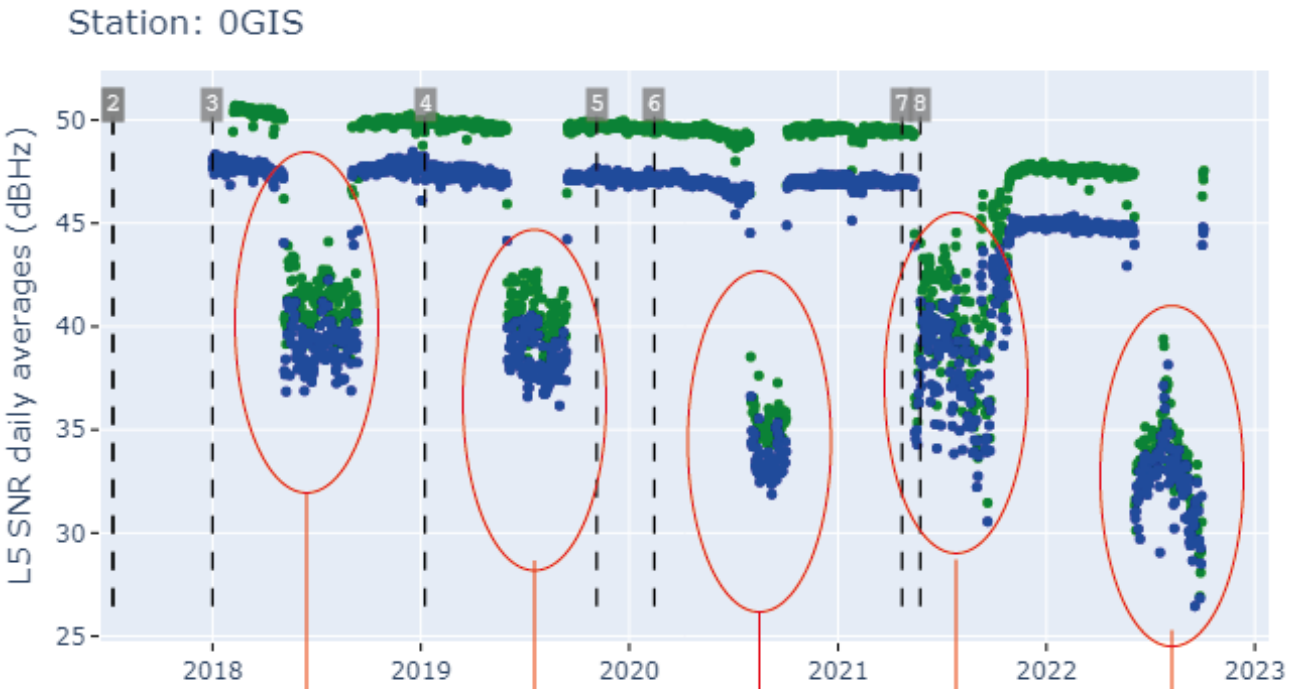


Key points of the detection system:

- In the presence of interference
  - Noise level increases, results in SNR drops
  - SNR are correlated among tracked satellites
    - SNR drops due to signal attenuation e.g., by trees and ionospheric scintillations won't be correlated among simultaneously tracked satellites
- Demonstration of the above points with simulated interference waves

RFI-related disturbances

Real signal interference incidents at Grisselhamn (0GIS)



2018:
Started - May 6
Stopped - September 13

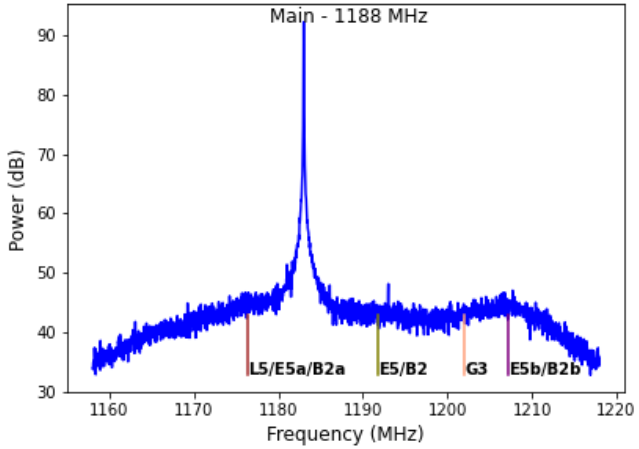
2019:
Started - June 1
Stopped - September 14

2020:
Started - July 31
Stopped - October 3

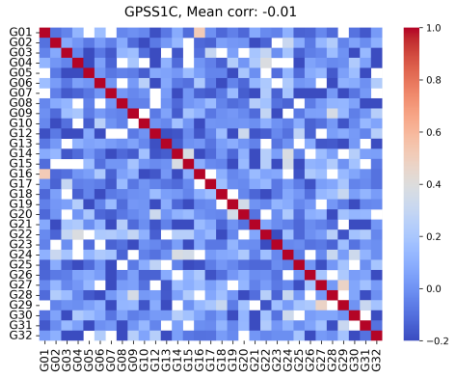
2021:
Started - May 15
Stopped - October 26

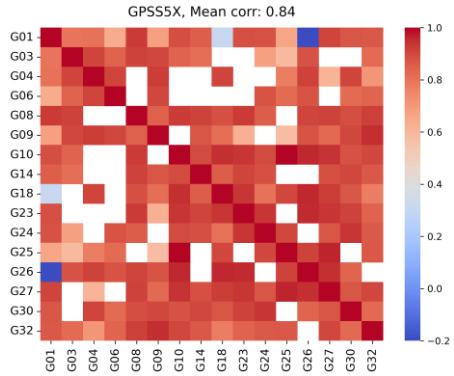
2022:
Started - June 4
Stopped - October 1

PTS located the source to be a boat.
The boat left the port on 1 October.
The disturbance has since ceased.
The source seems that same boat coming every year.
PTS will follow up for more information on the equipment



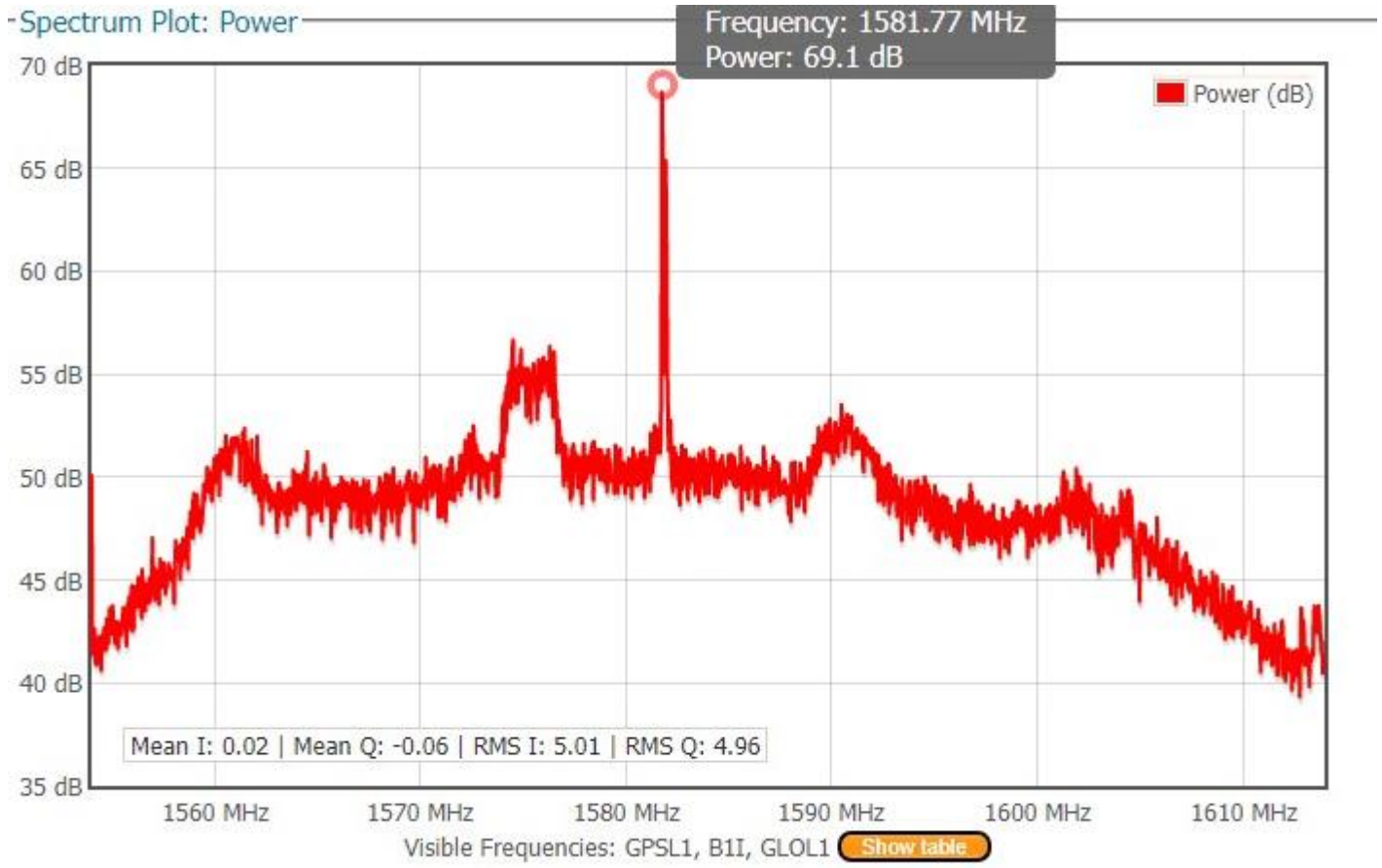
- RFI centered at 1181.0 MHz, but affected a wideband (-5 MHz to +26 MHz)





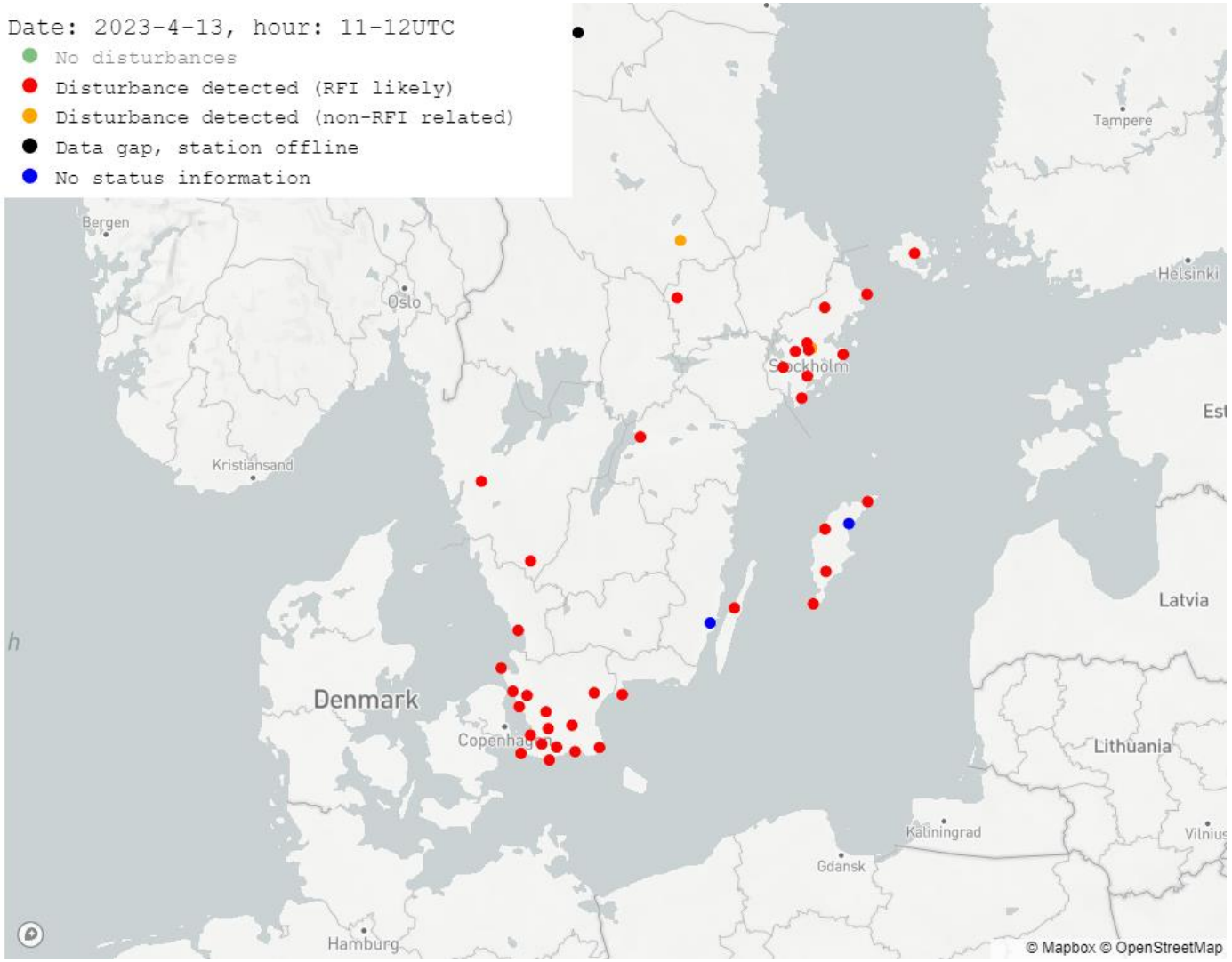
L1 disturbance – source located and contained

- RFI centered at 1581 MHz (~L1)
- 20-30 dBHz above the noise floor
- 5-6 MHz away from L1 center
- Affected GPS/GLO/GAL L1
- Detected at more than one station.
- Didn't have a major import on the performance of the station
- Source was located and contained, GPS repeater in a lab



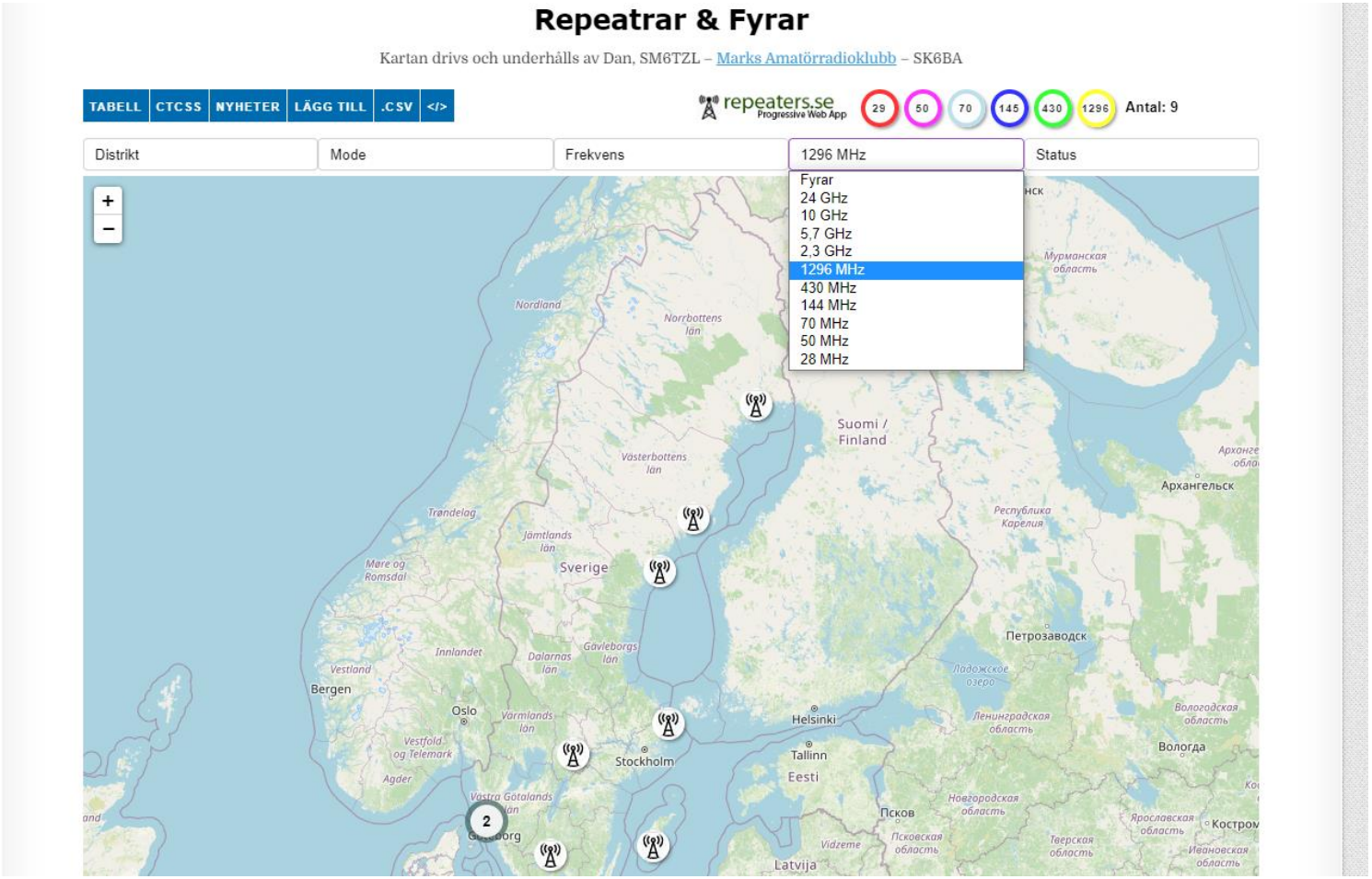
RFI Regional disturbance

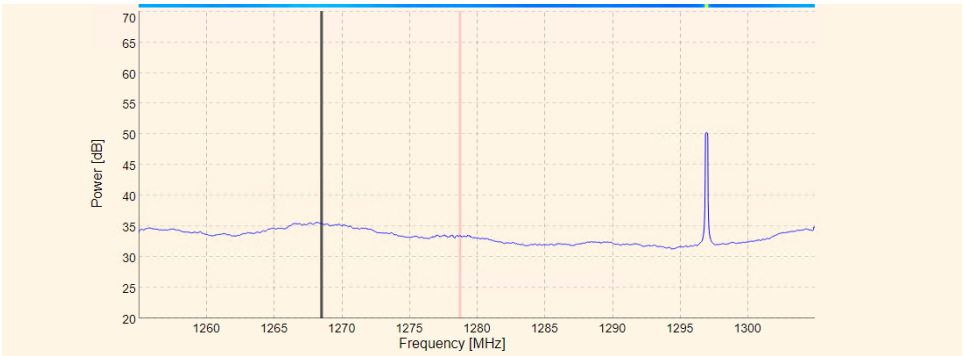
- RFI centered at 1260, and1325 MHz
- Affected GPS/GLO L2, BDS B3, Galileo E6
- Detected by several stations simultaneously
- Negligible impact on users
- PTS confirmed/detected the interference

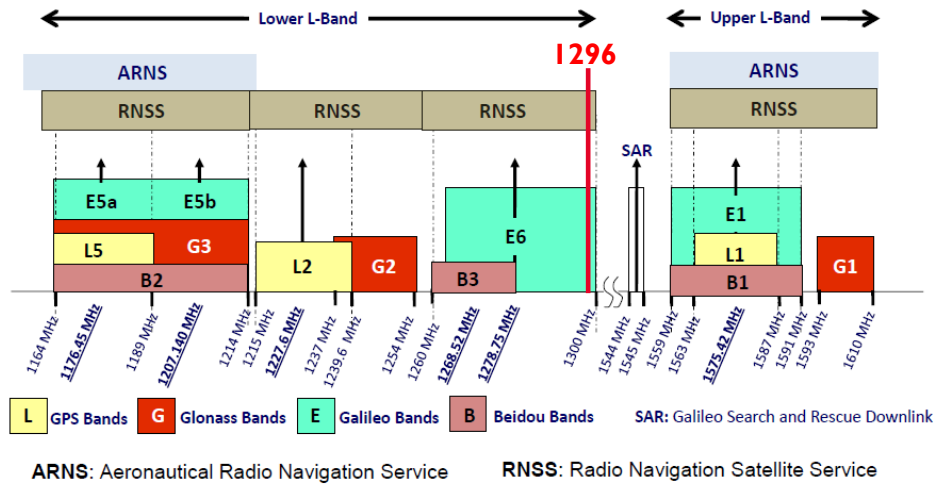


Radio Amateurs – Beacons at 1296, affecting Gal E6

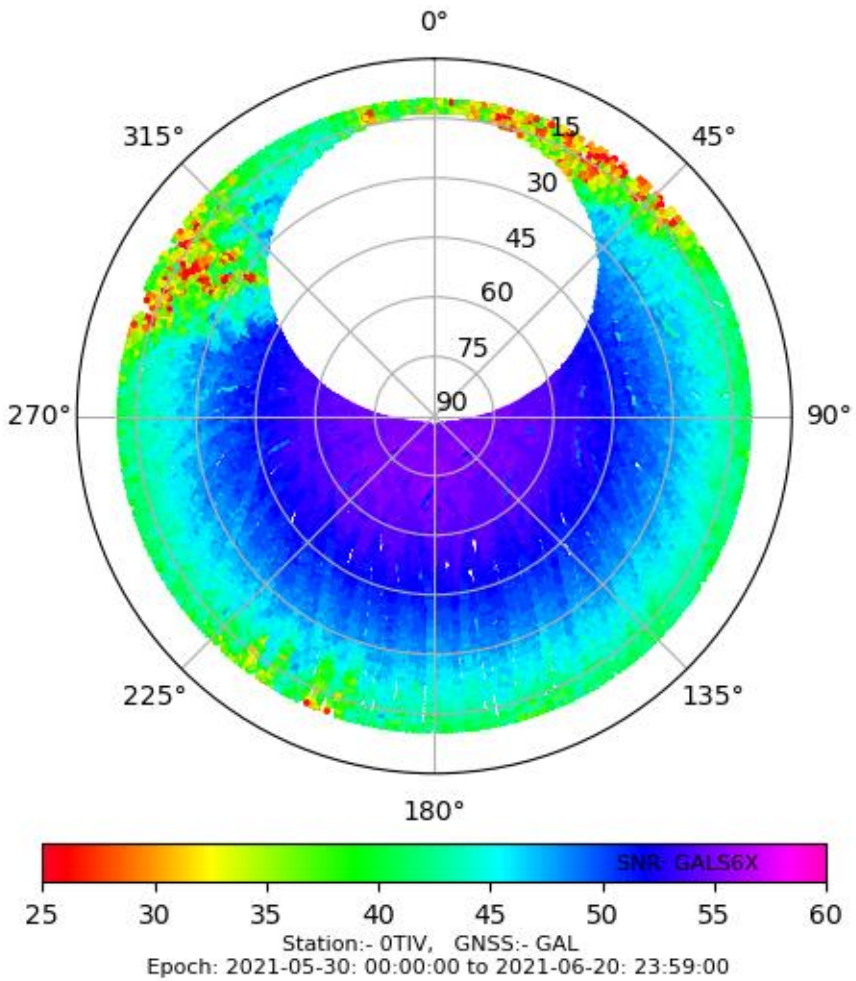
- Six SWEPOS stations affected
- Why affecting Galileo E6?
  - E6 transmission can extend to 1296
- B3 is also slightly affected

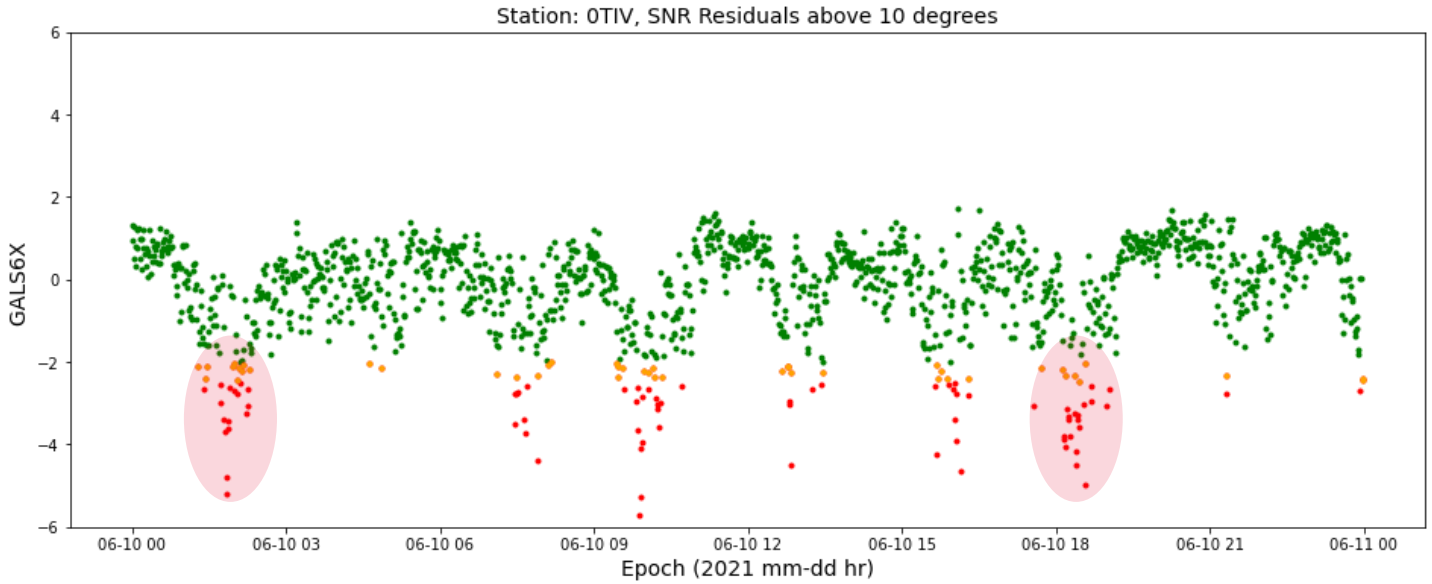


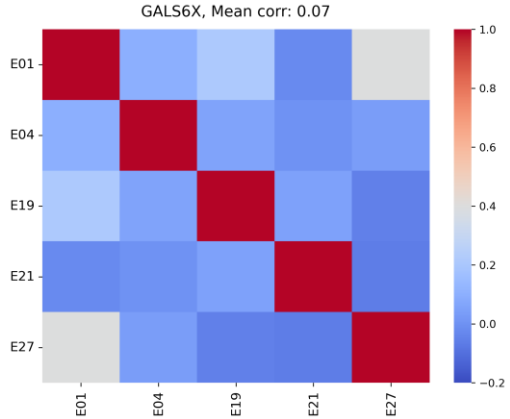


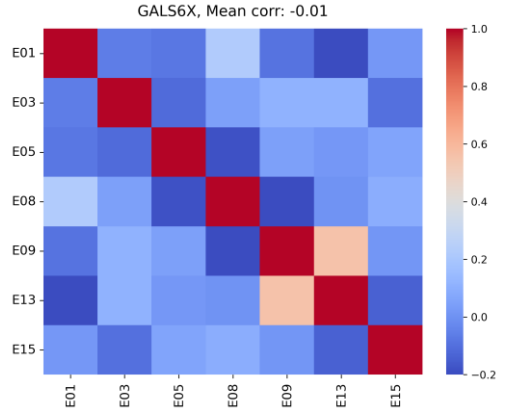


Non-RFI – Tree foliage attenuation







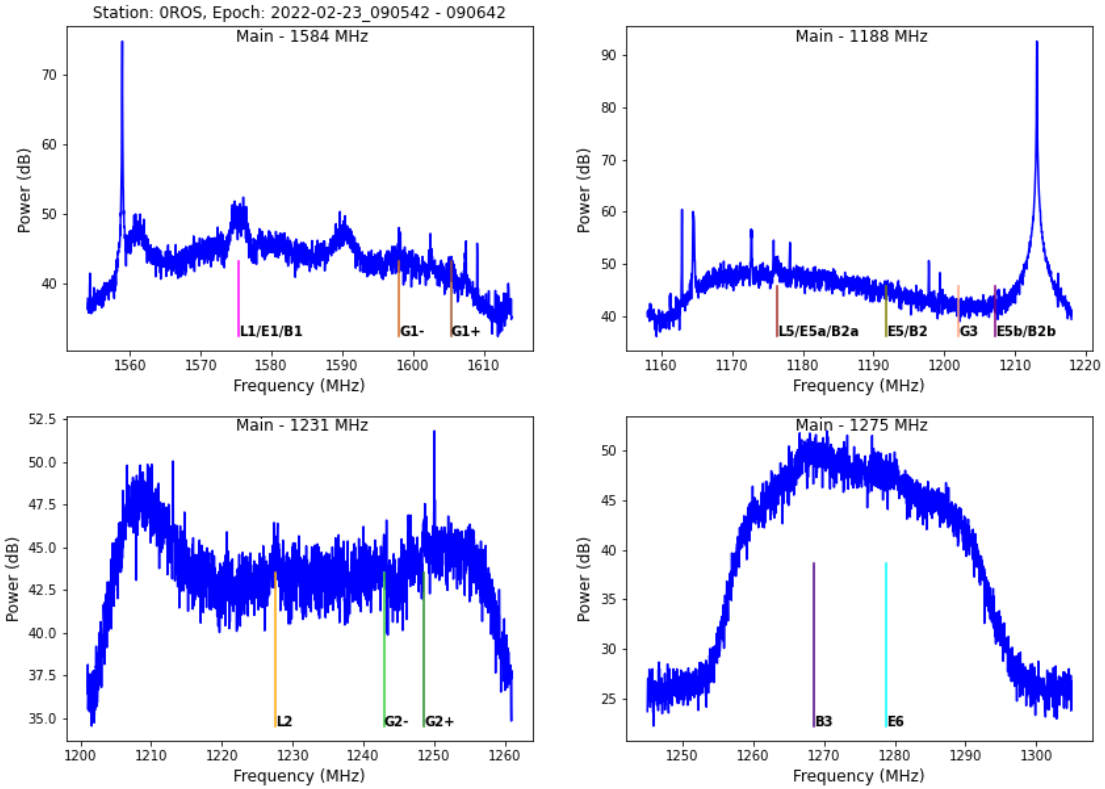


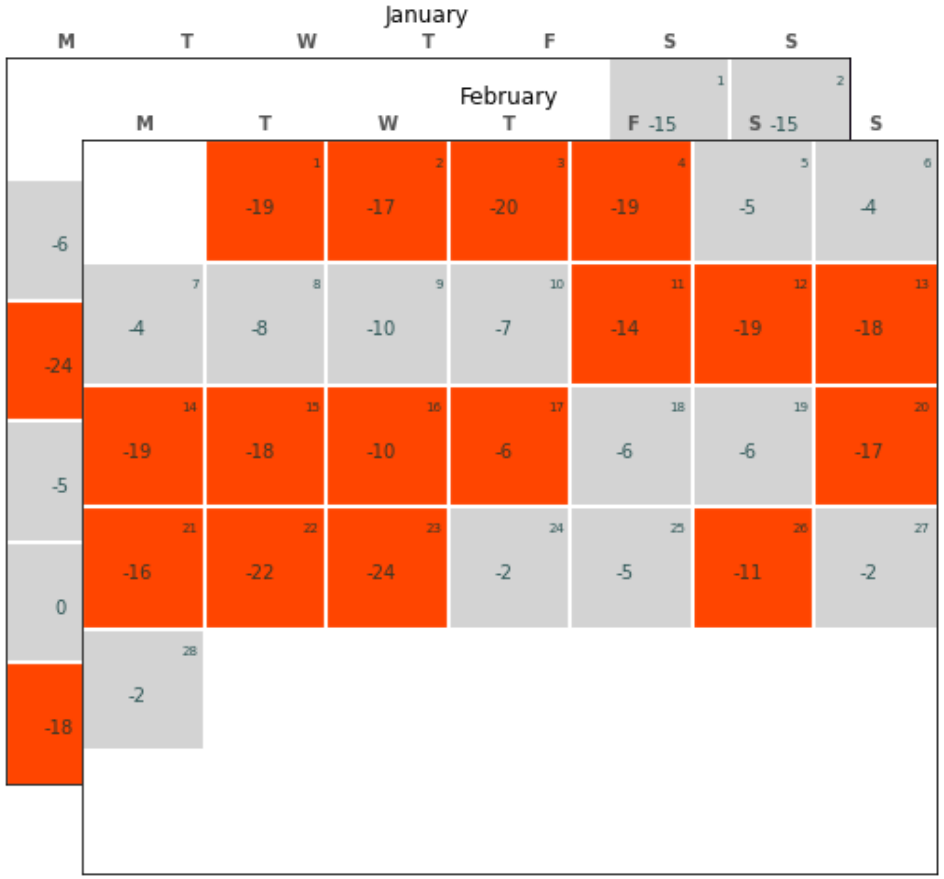
- Affects all signals
- Directional – In a certain azimuth
- Spectrum shows nothing
- SNR drops not correlated across satellites

Non-RFI – Equipment related disturbances

Rosvik (0ROS) – GPS L5, GAL E5/E5a/E5b, BDS B2a disturbances

- No L5 band signals tracked
- No Galileo satellites tracked
- Disturbances appear during cold days
- Antenna issue (TRM59800.00 → LEIAR20)





Takeaway!

- Hostile cyber operations on GNSS and GNSS-dependent infrastructures are a growing concern

- Monitor-Detect-Respond
  - GNSS dependent infrastructures should have a clear plan of recovering their system in the event of large-scale attacks and have other alternatives.
  - The goal is to protect critical GNSS and GNSS-dependent infrastructures against emerging (un)intentional threats; we should also use the same infrastructure for autonomous signal-situation awareness of threats.
  - Receiver and antenna manufacturers should consider interference threats when developing high-end GNSS receivers.
    - Users should make this part of a procurement when making receiver/antenna purchases