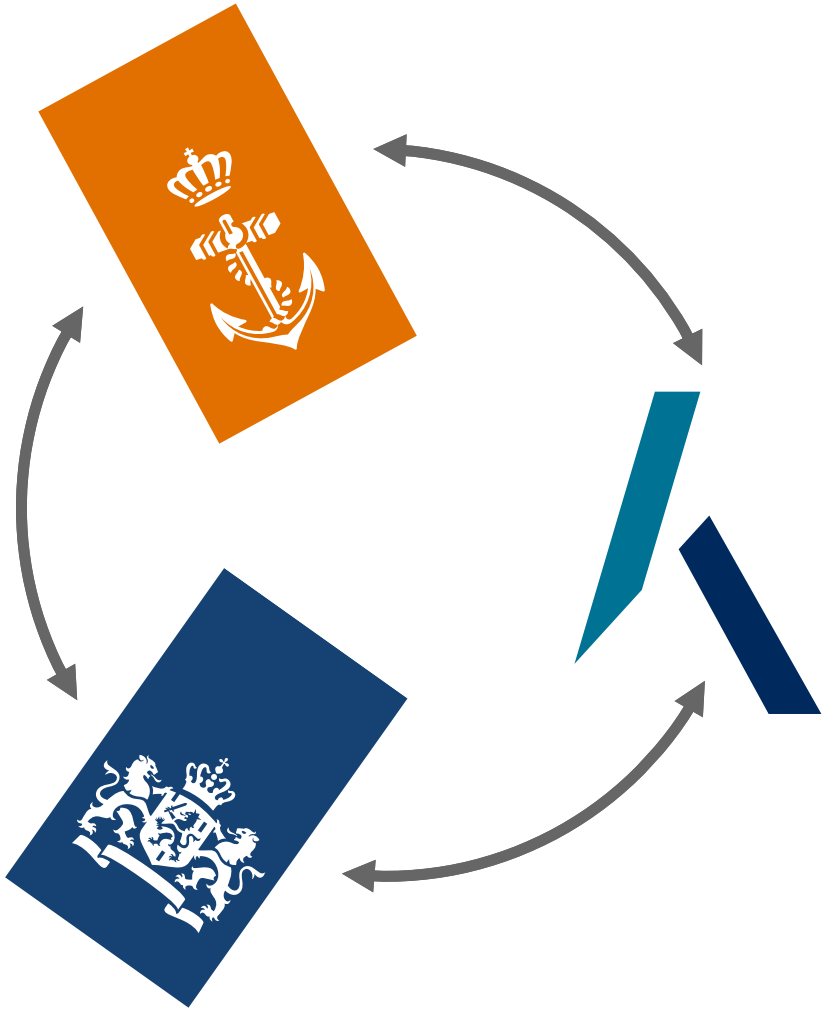


GNSS Interference from space as a catalyst for nationwide monitoring?

Lennard Huisman – NSGI

12th EUPOS® Council and Technical Meeting
Warsaw2026

Outline

- Current PNT monitoring based on GNSS network
- GNSS interference from space in our network

Current PNT monitoring based on GNSS network

- Interference and jamming is considered a threat, but no significant issues yet
- Proof of concept activities
- Currently mainly knowledge exchange with other capable organizations and stakeholders

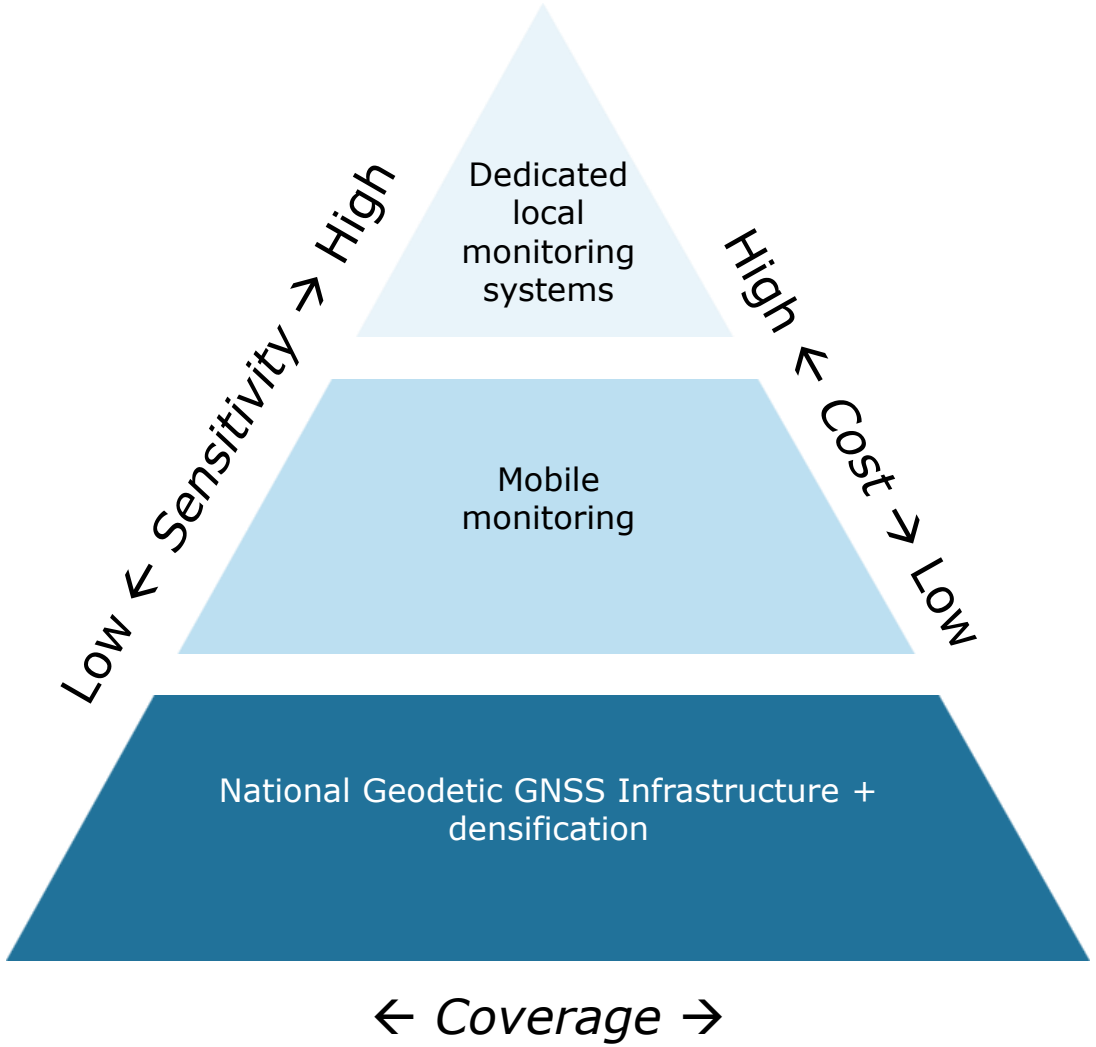
Hybrid PNT monitoring model

- Based on activites in other countries:
  - National projects
  - EUREF/EUPOS examples
  - Literature
- Need for:
  - local monitoring at critical locations (airports, harbour, events, …)
  - Mobile monitoring to pinpoint sources
  - Nationwide monitoring for large scale events

- How to convince key players of added value of national GNSS stations?

→ We need to show it works:

Clements and Humphreys!



Public awareness

https://www.youtube.com/watch?v=tz23G_UXCGA

YouTube NL

Zoeken

Something is jamming GPS over Europe. Here's what we found

Veritasium
21,3 mln. abonnees

Abonneren

292K | Delen | Opslaan

arXiv:2606.03673v1 [eess.SP] 2 Jun 2026

Chasing Lightning: Detecting, Characterizing, and Identifying a Powerful Space-Based GNSS Interference Source

Zachary L. Clements*, Argyris Kriezis†, and Todd E. Humphreys*
* *Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin*
† *Department of Aeronautics and Astronautics, Stanford University*

ABSTRACT

This paper analyzes and identifies a space-based Global Navigation Satellite System (GNSS) interference source that has caused scores of powerful transient wide-area interference events over continental Europe, Greenland, and Canada since 2019. While terrestrial or near-terrestrial sources are primarily responsible for the recent uptick in GNSS interference worldwide, space-based interferers are of special concern given their potential for vast geographic reach and their portent of a qualitative escalation in GNSS interference. Based on data collected between 2019 and 2026 from a network of terrestrial GNSS reference stations, this paper (1) develops a received-power-based detection framework; (2) details the spatial, temporal, and spectral patterns of wide-area interference events caused by the source; (3) presents and analyzes identification techniques that blend received-power and time-difference-of-arrival measurements; and (4) applies these techniques to confidently identify the GNSS interference source as a constellation of Russian early warning satellites in Molniya ("lightning") orbits.

1 INTRODUCTION

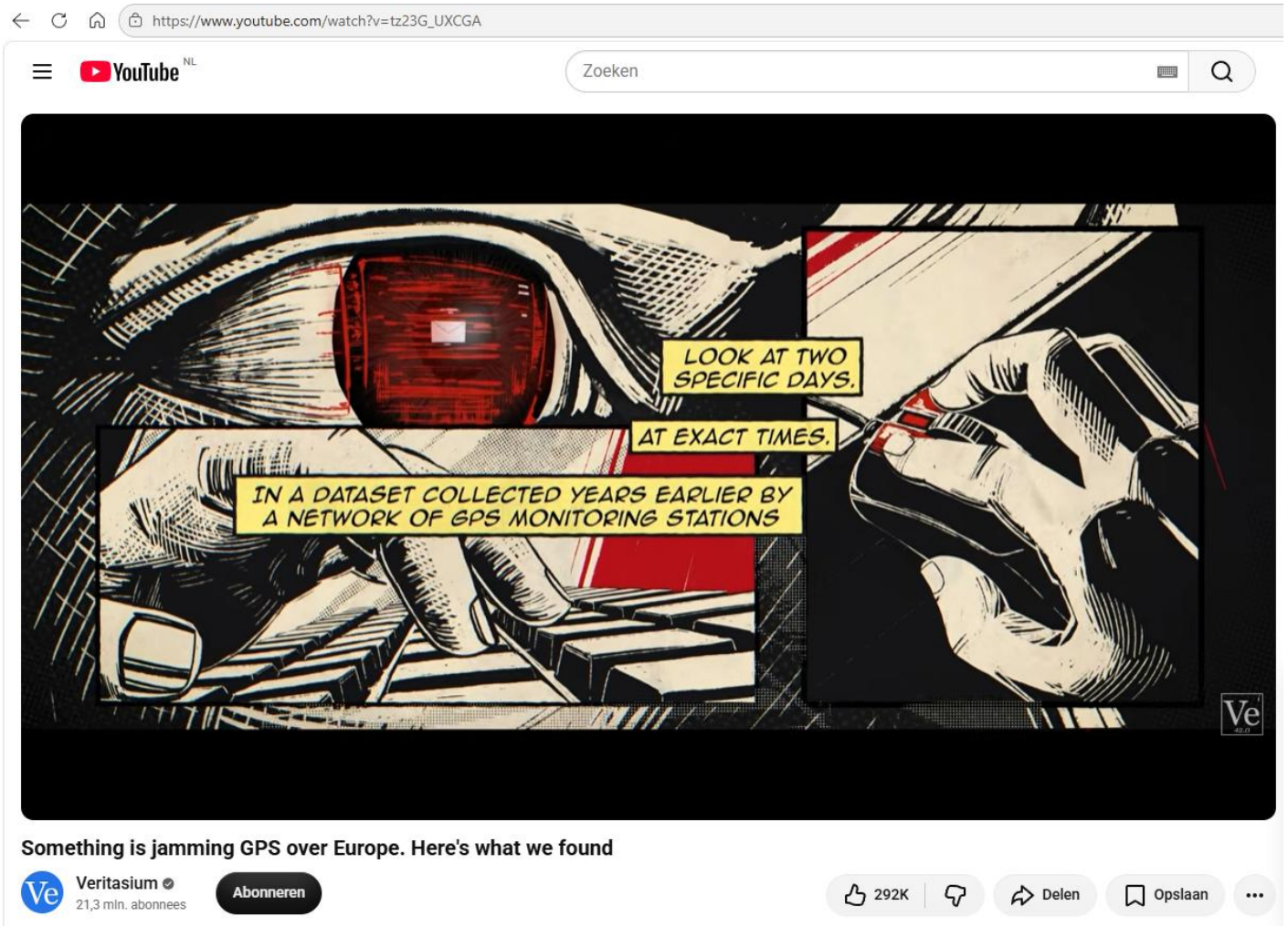
Global Navigation Satellite Systems (GNSS) such as GPS provide meter-accurate positioning while offering global accessibility and all-weather, radio-silent operation. However, GNSS is fragile: its service is easily degraded by both deliberate (e.g., jamming and spoofing) and naturally occurring (e.g., multipath and atmospheric) interference (Scott, 2003; Humphreys et al., 2008; Humphreys, 2012, 2017). The past five years have seen a crescendo of GNSS disruptions in the aviation and maritime sectors (Osechas et al., 2022; GPS Spoofing Workgroup, 2024; Marcos et al., 2018; RIN Maritime GNSS Interference Working Group, 2026). Interference is especially problematic in these fields because GNSS is deeply interwoven into critical systems. Beyond simple navigational or timing displacement, cascading failures can occur when GNSS loss or corruption triggers follow-on problems in downstream systems (GPS Spoofing Workgroup, 2024; RIN Maritime GNSS Interference Working Group, 2026).

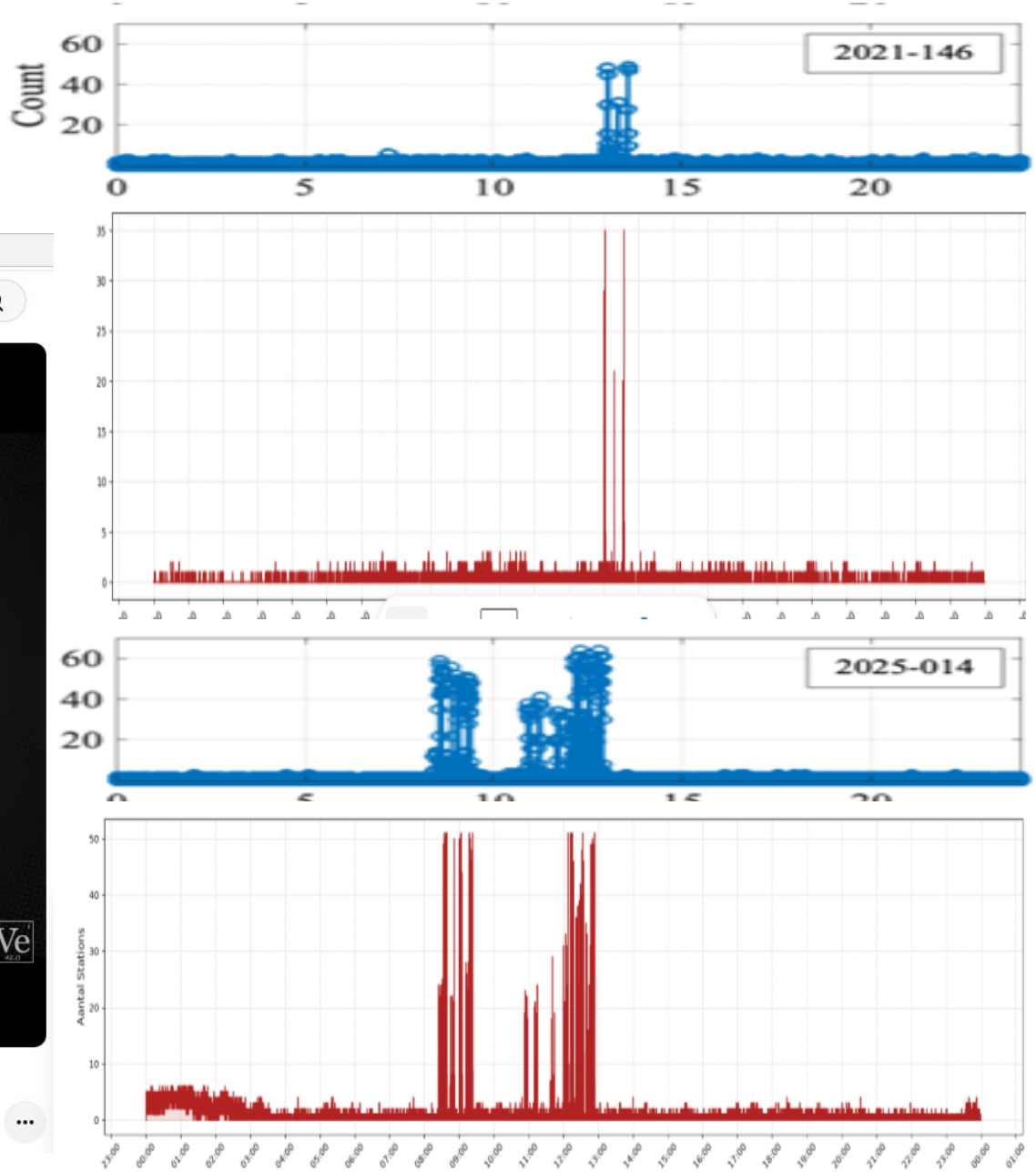
Fortunately, significant progress has been made over the past decades in GNSS interference mitigation and countermeasures (Psiaki and Humphreys, 2016, 2020; Borio et al., 2012; Clements et al., 2022). It has been shown that dedicated GNSS interference monitoring systems provide valuable spectrum situational awareness to enhance navigation security (Gunawardena et al., 2009; Gunawardena and Van Graas, 2011; Stader and Gunawardena, 2021; Kriezis et al., 2024; Sokolova et al., 2022; Morrison et al., 2023), with some demonstrating the ability to geolocate the interference source (Bhatti et al., 2012; Mitch et al., 2016). Furthermore, GNSS receivers situated in LEO enable terrestrial GNSS interference detection, characterization, and geolocation with worldwide coverage (Murrian et al., 2021; Clements et al., 2023, 2026).

Networks of terrestrial GNSS receivers can also be enlisted for GNSS interference monitoring (Abraha et al., 2024), including of space-based interference. York et al. (2014) revealed that GPS PRNs 24 and 27 (SVN65 and SVN66) were transmitting leakage tones at ±10 MHz and ±20 MHz from the GPS L5 frequency. The anomaly was subsequently fixed. More recently, a network of terrestrial reference stations was used to identify a BeiDou satellite (NORAD ID 40749) as a source of interference in the B3I band (1268.52 MHz) (Patil et al., 2023, 2024). The offending satellite continuously transmitted a tone centered at 1268.52 MHz and tones at ±10 MHz and ±20 MHz from this frequency. These tones are no longer present at the time of writing. Both of these interference cases were apparently due to faulty or improperly configured hardware.

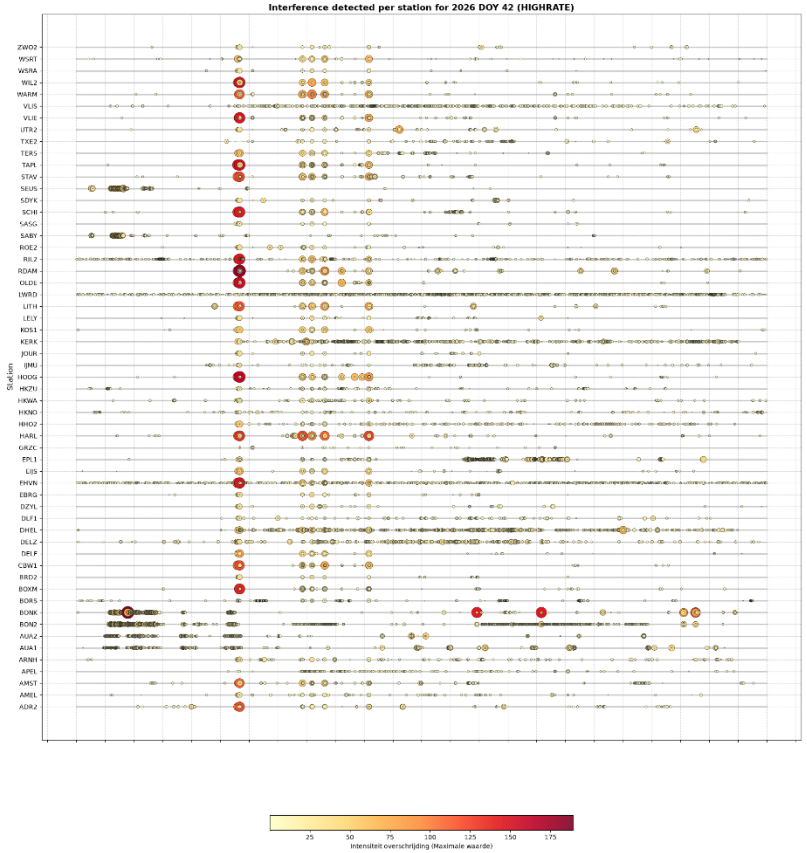
This paper reports on the detection, characterization, and source identification of powerful transient GNSS interference originating from a non-GNSS satellite. The phenomenon was briefly mentioned in European Space Agency NAVISP-EL3-014 (2023), and more fully characterized in a preliminary conference publication by the current authors, Clements and Humphreys (2025). The current paper significantly extends both works. The interference reported here is different from that detailed in Patil et al. (2023, 2024); York et al. (2014) in several respects: (1) it is transient rather than continuous—the duration of interference events is less than 10 seconds; (2) it affects signals in the widely used GPS L1 frequency band rather than the less-common L5 and B3I bands; (3) it is much more powerful, causing drops in terrestrial receiver carrier-to-noise ratios (CNRs) of up to 10 dB; and

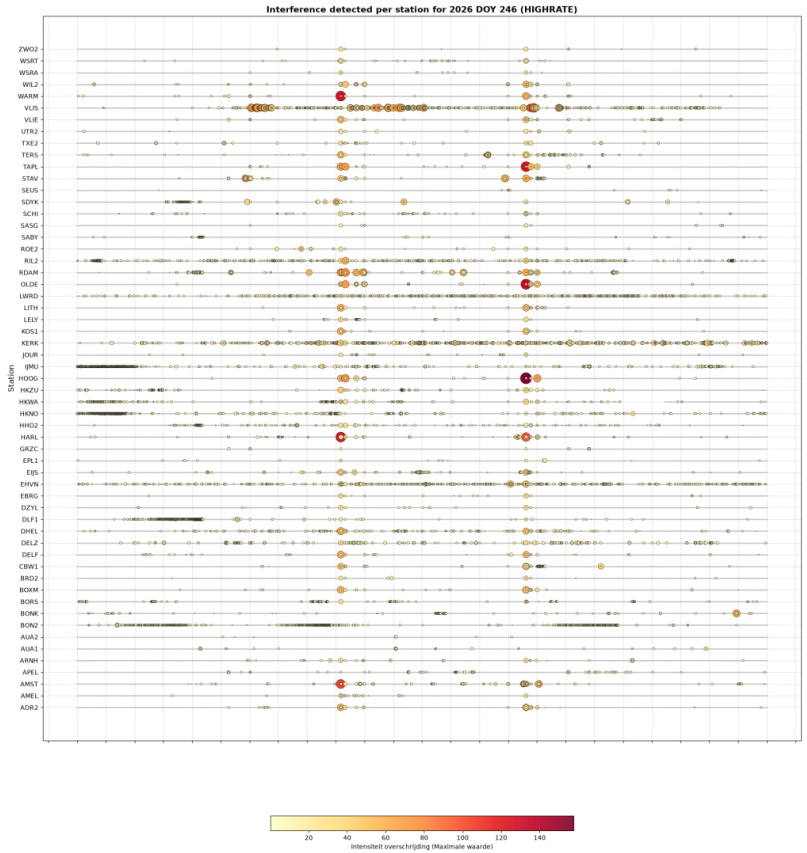
Public awareness





Impact NLD GNSS network





Impact NLD GNSS network

https://gpspatron.com/satellite-gps-galileo-interference-europe/

GPSPATRON

Detected by GPSPATRON Sensors and GP-Cloud Across Europe

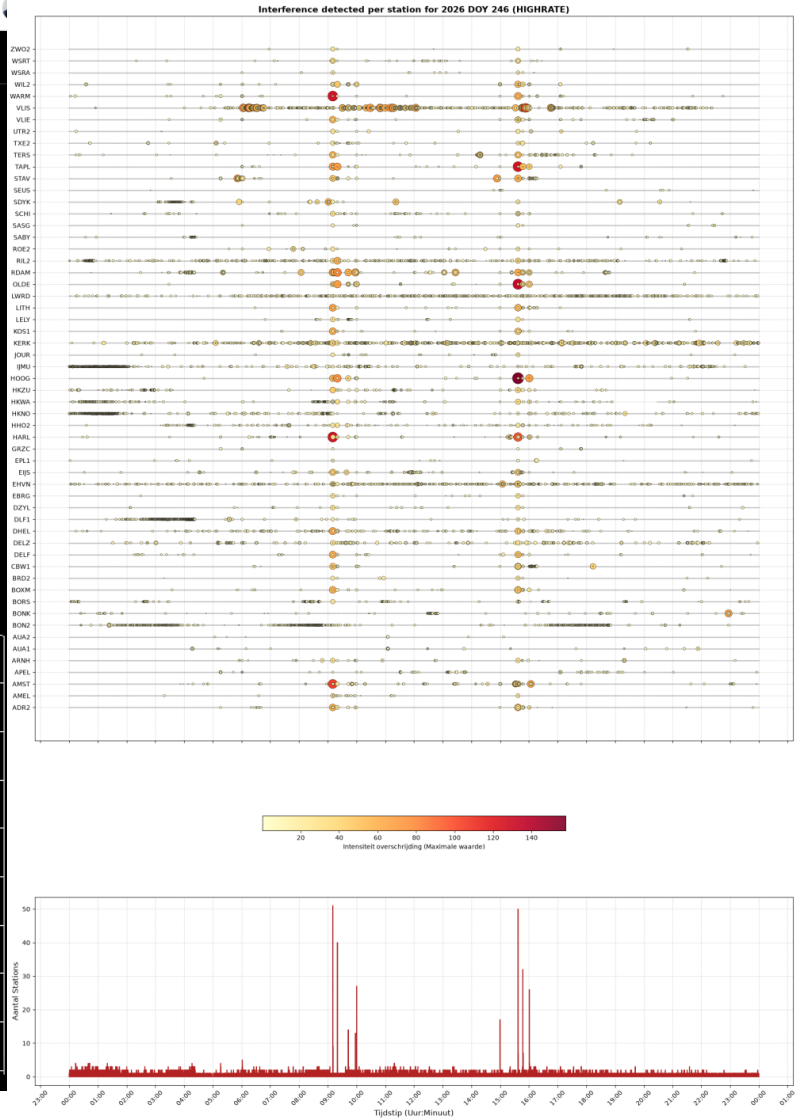
The same interference was recorded by multiple independent GNSS data sources and sensor types within the GPSPATRON monitoring infrastructure. These included RTK reference stations connected via RTCM@NTRIP, Septentrio receivers connected via SBF@NTRIP, GP-Probe DIN L1, and GP-Probe TGE2 interference detectors.

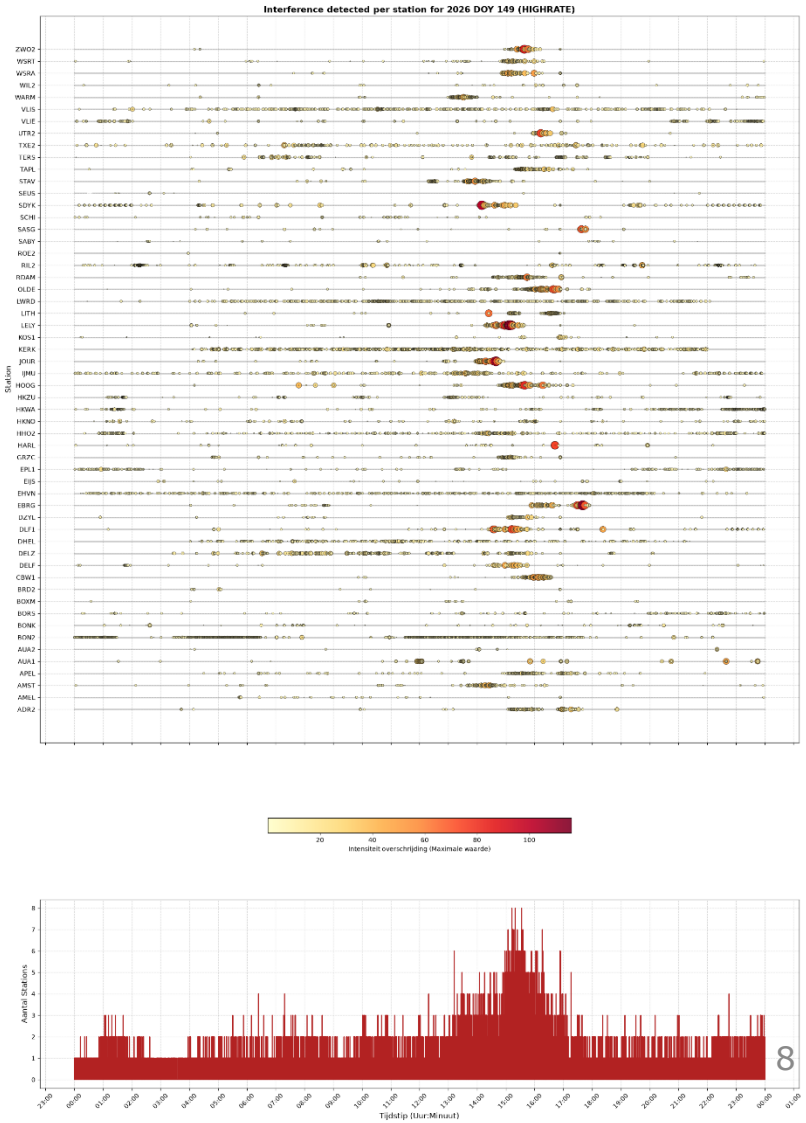
This cross-platform consistency is important because the devices differ in RF front ends, GNSS receivers, antennas, installation environments, and data-processing methods. Nevertheless, they all showed the same short disturbance at the same time. GP-Cloud automatically detected the RF anomaly and classified it as jamming affecting GPS and Galileo.

Across the affected monitoring points, the event produced a measurable reduction in carrier-to-noise density, with C/N₀ decreasing by approximately 2 to 5 dB-Hz depending on the receiver and location.

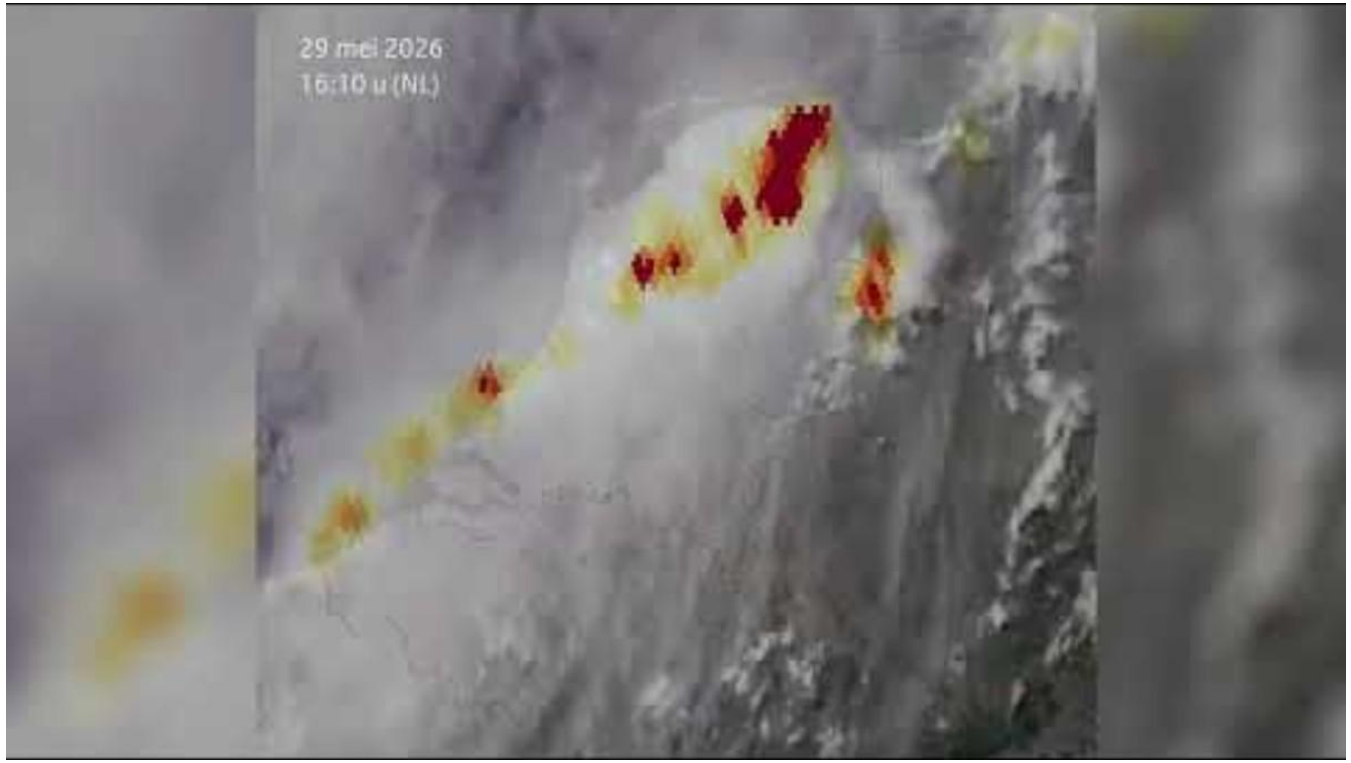
Event Overview

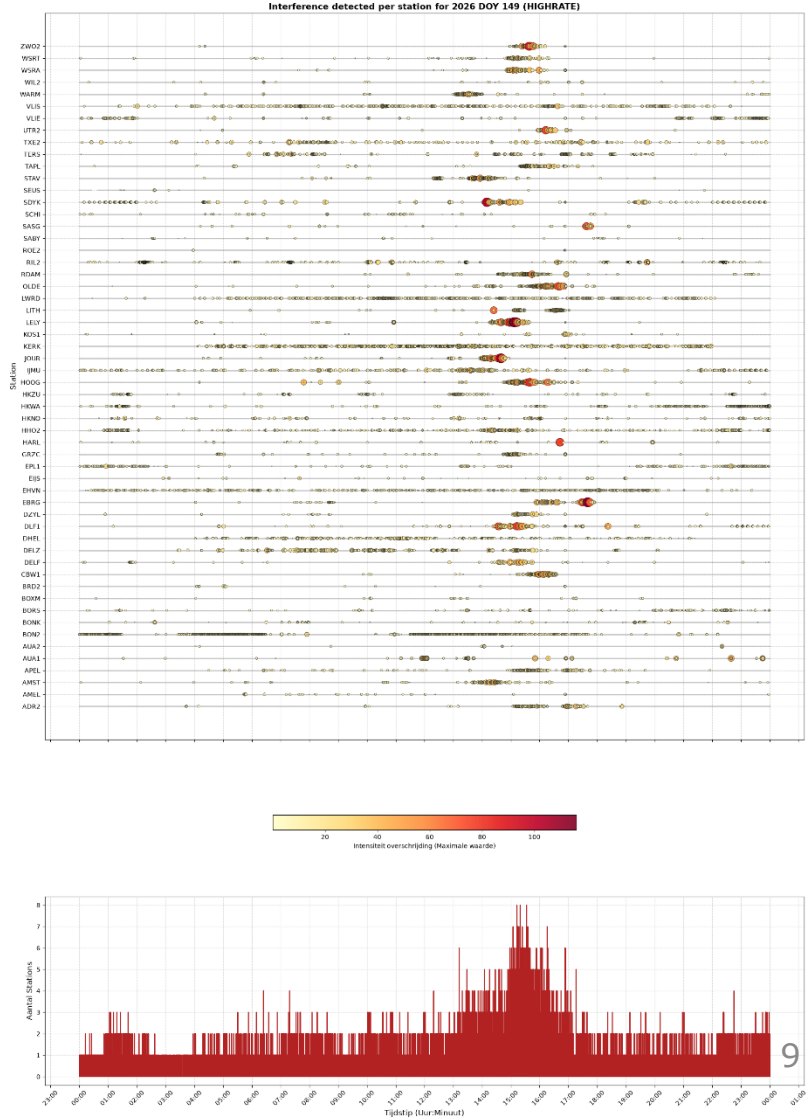
Parameter	Observation
Date	3 September 2026
Approximate time	Around 09:10 UTC
Event duration	A few seconds
Geographic coverage	Across Europe, from Poland to the United Kingdom
Sensor types	RTK stations, Septentrio receivers, GP-Probe DIN L1, GP-Probe TGE2
GNSS affected	GPS and Galileo
Automatic classification	Jamming
Observed C/N₀ degradation	Approximately 2–5 dB-Hz





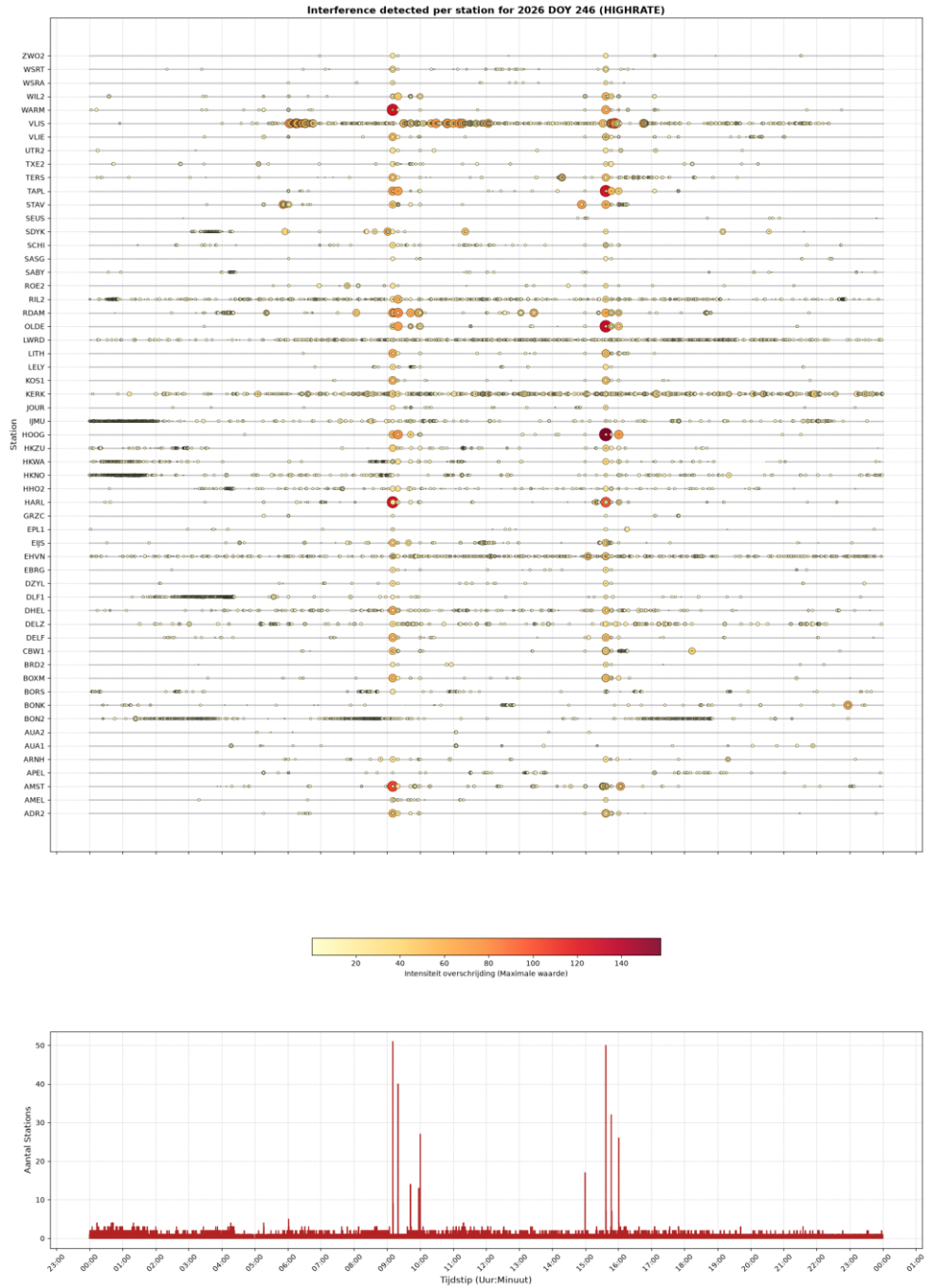
Impact NLD GNSS network

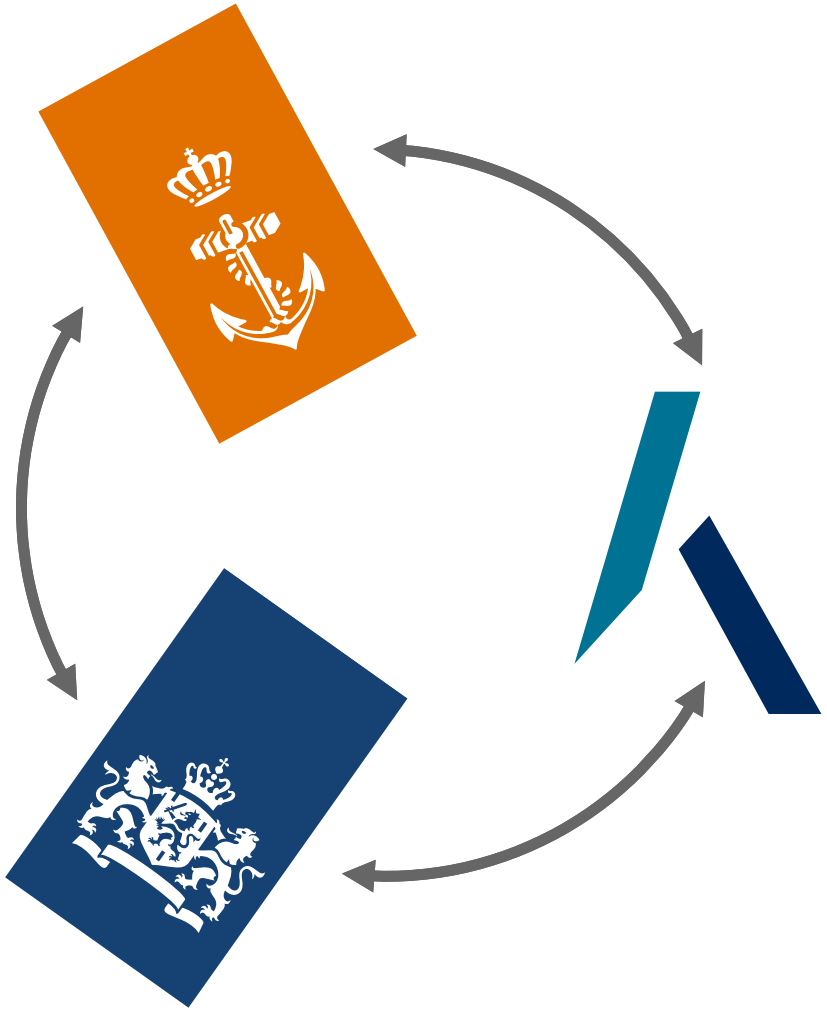




Summary

- National coordination on monitoring activities in start-up phase
- We focus on showing the value of our data
- Public awareness on jamming from space is an opportunity?
- Many occurrences detected in 2026
- Still many thing to consider
  - Hardware dependencies
  - Critical values
  - Alerting
  - …





GNSS Interference from space as a catalyst for nationwide monitoring?

Lennard Huisman – NSGI

12th EUPOS® Council and Technical Meeting
Warsaw2026