BALTIC SEA GNSS INTERFERENCE

REVEALED BY TECHNOLOGY OF GPSPATRON DURING JUNE THROUGH NOVEMBER 2024

cyntony corporation

An explainer for position, navigation and timing practitioners by GNSS Cybersecurity experts GPSPATRON and Gdynia Maritime University, Poland. Published by permission. Cyntony Corporation is authorized North America distributor of GPSPATRON Sp. z o.o.

Report on GNSS Interference in the Baltic Sea: Analysis Using a Terrestrial Monitoring System and Comparison with ADS-B Data

Observation period:
02.JUN.2024 - 28.NOV.2024

Date: 11.02.2025 Doc. revision: 2.1

GPSPATRON
Poland

Contact person:
Maksim Barodzka, CEO
mb@gpspatron.com
+48 516 108 888

www.gpspatron.com

Gdynia Maritime University
Poland

Contact person:
Jaroslaw Cydejko PhD, Eng,
Master Mariner
Faculty of Navigation,
j.cydejko@wn.umg.edu.pl

https://umg.edu.pl/en/

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Executive Summary

GNSS interference has become a significant issue in the Baltic Sea, with daily detections observed in ADS-B data from aircraft. However, existing studies primarily focus on high-altitude interference, leaving a critical gap in understanding its impact on ground-based infrastructure. This report presents a comprehensive six-month analysis of terrestrial GNSS interference monitoring, conducted by GPSPATRON in collaboration with Gdynia Maritime University.

Our study deployed a GP-Probe TGE2-CH3 4G RFSA sensor at Gdynia Maritime University to detect and analyze interference events affecting GNSS signals at ground level. The collected data was processed in real-time through GP-Cloud, enabling detailed statistical assessments and comparison with airborne ADS-B interference data.

Key Findings:

- **84 hours** of GNSS interference detected, with the majority attributed to jamming signals rather than spoofing.
- Peak interference activity was recorded in October, with six separate jamming incidents, totaling **29 hours of disruptions**—the highest level observed during the study.
- Two distinct interference types were identified:
    - Multi-constellation jamming, observed predominantly from June to September.
    - Multi-tone interference, first detected in October, indicating a shift in jamming techniques.
- No clear correlation was found between terrestrial GNSS interference and **ADS-B-based** interference detection, reinforcing the limitations of high-altitude monitoring in assessing ground-level threats.
- The interference likely originated from a mobile maritime source, given its periodic occurrence and movement patterns.
- Some interference events led to significant positioning errors, degrading accuracy from 3–5 meters to over **35 meters**—posing a serious risk to navigation, port operations, and critical infrastructure.
- Long-duration interference events, some exceeding **7 hours**, indicate persistent GNSS disruption, significantly affecting positioning and timing applications.

Conclusion & Recommendations:

This study highlights the urgent need for a dedicated GNSS interference monitoring network along the Baltic Sea coast. Relying solely on ADS-B-based interference detection systems is insufficient for assessing GNSS interference threats to **ground-based infrastructure** and may even create a false sense of security among infrastructure operators. Since ADS-B-based analysis services report daily interference detections, some operators assume that these threats are well understood and do not pose a direct risk to their systems. This misconception is dangerous, as it

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

obscures the reality that ground-level GNSS interference can have severe operational impacts while remaining undetected in high-altitude monitoring datasets.

To effectively address this issue, a **terrestrial GNSS interference monitoring** network with **TDOA-based geolocation** capabilities should be established. Such a system would provide real-time tracking of interference sources, facilitate regulatory enforcement, and enhance the protection of critical GNSS-dependent infrastructure. By delivering precise, localized data, a dedicated monitoring network would bridge the gap between airborne and ground-based interference assessments, ensuring that infrastructure operators and regulatory bodies have an accurate understanding of the threat landscape.

The findings of this study underscore the increasing risks of GNSS interference and the pressing need for proactive countermeasures to safeguard navigation, communication, and security systems across the Baltic region.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

1. Introduction

Existing studies on GNSS interference in the Baltic Sea region predominantly rely on ADS-B data from aircraft, which provide valuable insights into interference patterns at cruising altitudes and their impact on aviation. However, these datasets are not directly applicable to assessing GNSS interference at ground level, where the majority of critical infrastructure is located. The fundamental differences in propagation conditions between high-altitude and ground-based environments—caused by factors such as the curvature of the Earth, and RF signal propagation conditions—result in significantly different interference characteristics. GNSS jamming and spoofing signals that are detectable at high altitudes may not have a measurable impact on terrestrial systems, while low-power interference sources that disrupt ground-based GNSS receivers may remain undetected in ADS-B-based studies. Consequently, airborne monitoring does not provide a comprehensive assessment of the interference risks faced by ground infrastructure.

To address this gap, our study aims to characterize the statistical properties of GNSS interference at ground level and quantify the occurrence of interference events affecting terrestrial infrastructure. As of today, there are no publicly available studies that systematically examine GNSS interference in this context. The collection and analysis of ground-level GNSS interference data remain significantly underrepresented in existing monitoring frameworks, which largely focus on high-altitude detection methodologies (e.g., gpsjam.org, spoofing.skai-data-services.com, flightradar24).

This study represents the first phase of our research conducted in collaboration with Gdynia Maritime University. Our primary objective was to obtain baseline statistical data on GNSS interference at ground level and compare these findings with interference observed at high altitudes. To achieve this, we installed a single GP-Probe TGE2-CH3 4G RFSA sensor on the third floor of the Faculty of Navigation building at Gdynia Maritime University, where it continuously monitored GNSS signal quality and detected interference events.

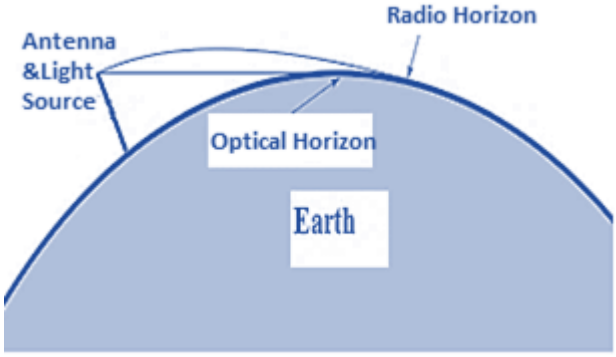
The collected data was transmitted in real-time to GP-Cloud, enabling subsequent joint analysis with Gdynia Maritime University. By examining the interference patterns detected at ground level and comparing them to airborne observations, we aimed to assess potential differences in signal impact across varying altitudes. The findings from this study provide valuable insights into the characteristics and prevalence of GNSS interference at ground level, offering a more accurate understanding of its implications for maritime navigation, port operations, and other GNSS-dependent infrastructure in the region.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

2. Potential Risks of GNSS Interference for Ground-Based Infrastructure

It is widely recognized that the Baltic Sea region is extensively affected by GNSS interference, with daily detections based on ADS-B data from aircraft. However, there are no publicly available reports or datasets indicating that these interference events have a direct impact on critical ground-based infrastructure. This could lead to a misconception that GNSS interference does not pose a significant threat to terrestrial critical infrastructure, which is not the case.

The fundamental issue lies in the physics of RF signal propagation. Due to the curvature of the Earth, the radio horizon for GNSS L1 signals, when received by an antenna placed at a height of 50 meters, is approximately 35 km.



Kumar, Suresh & Ramachandran, Rajesh. (2018). The Quantum Key Distribution, Attenuation and Propagation over Ocean Surface for Various Naval Applications. International Journal of Scientific Research in Network Security and Communication. 6. 10.26438/ijsrnsc/v6i2.5461.

This means that even if a large portion of the Baltic region appears to be affected by strong GNSS interference based on ADS-B data, these signals may not propagate effectively to the ground and thus may have little to no direct impact on terrestrial systems. Conversely, low-power jamming and especially spoofing signals, which may not be strong enough to disrupt GNSS reception at high altitudes, can significantly affect ground-based receivers and critical infrastructure, yet remain undetected in ADS-B-based studies.

GNSS interference can cause a range of operational problems for critical infrastructure, including:

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

- **Maritime Navigation** – GNSS is essential for precise positioning, route planning, collision avoidance, and e-navigation. Interference can lead to misnavigation, increased risk of groundings and collisions, and degraded situational awareness, particularly in congested waterways.
- **Port Operations** – Modern ports rely on GNSS for vessel berthing, automated container handling, and logistics management. Disruptions can delay cargo operations, impact crane automation, and hinder efficiency in port traffic control.
- **Construction and Offshore Engineering** – Precise GNSS positioning is critical for large-scale infrastructure projects, including offshore wind farms and subsea cable installations. Jamming and spoofing can cause misalignment of structures, delays, and economic losses.
- **Emergency Response and Search & Rescue** – GNSS is vital for maritime distress signals, coast guard coordination, and emergency response teams. Interference can lead to delayed response times and reduced effectiveness in locating and assisting vessels in distress.
- **Timing Synchronization in Telecommunications and Energy** – Many telecom networks (3G, 4G, SATCOM, PMR, PSTN) and power grid infrastructures rely on GNSS-based timing for synchronization. Disruptions can result in network instability, degraded service quality, and even cascading failures in energy distribution.
- **Financial Services** – Regulatory requirements such as MiFID II and SEC 613 mandate high-precision GNSS timestamps for financial transactions. GNSS disruptions can lead to timestamp inconsistencies, regulatory violations, and financial discrepancies.
- **Airports and Aviation Operations** – ICAO Annex 10 mandates the use of GNSS for aviation navigation and approach procedures. GNSS interference can cause navigation errors, affect automatic dependent surveillance systems, and lead to flight delays and rerouting.
- **Railway Systems** – Low-density railway networks depend on GNSS for train tracking, signaling, and control automation. Jamming or spoofing can cause incorrect positioning data, leading to potential train delays, misrouting, or even safety risks.
- **Network RTK (Real-Time Kinematic Positioning)** – RTK-based applications, including land surveying, precision agriculture, and autonomous machinery, require centimeter-level positioning accuracy. GNSS interference reduces reliability and precision, impacting productivity and operational efficiency.
- **Autonomous Machines and Drones** – Unmanned ground vehicles, aerial drones, and industrial automation systems rely on GNSS for accurate navigation and mission execution. Interference can result in system failures, unexpected deviations, or complete loss of control.
- **Dangerous Goods Transportation** – The secure transport of hazardous materials requires continuous GNSS-based tracking to ensure regulatory compliance and prevent unauthorized deviations. GNSS interference can compromise monitoring capabilities and pose security risks.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

- **Spectrum Monitoring and Regulatory Compliance** – GNSS is used for spectrum monitoring to detect unauthorized transmissions and interference sources. Disruptions can reduce the effectiveness of regulatory enforcement and frequency management.
- **Armed Forces and National Security** – Military forces rely on GNSS for strategic navigation, targeting, and situational awareness. Jamming and spoofing threats pose significant risks to operational effectiveness, particularly in conflict zones and defense applications.

Given these potential risks, ground-based GNSS interference monitoring is crucial for understanding the full extent of the problem and implementing mitigation strategies. In this study, we deployed a terrestrial monitoring system to collect long-term data on GNSS interference in the Baltic Sea, providing insights into the characteristics, frequency, and sources of disruptions at ground level. The findings help bridge the gap between airborne interference studies and the real challenges faced by infrastructure on the Earth's surface.

3. Measurement Setup and Data Acquisition

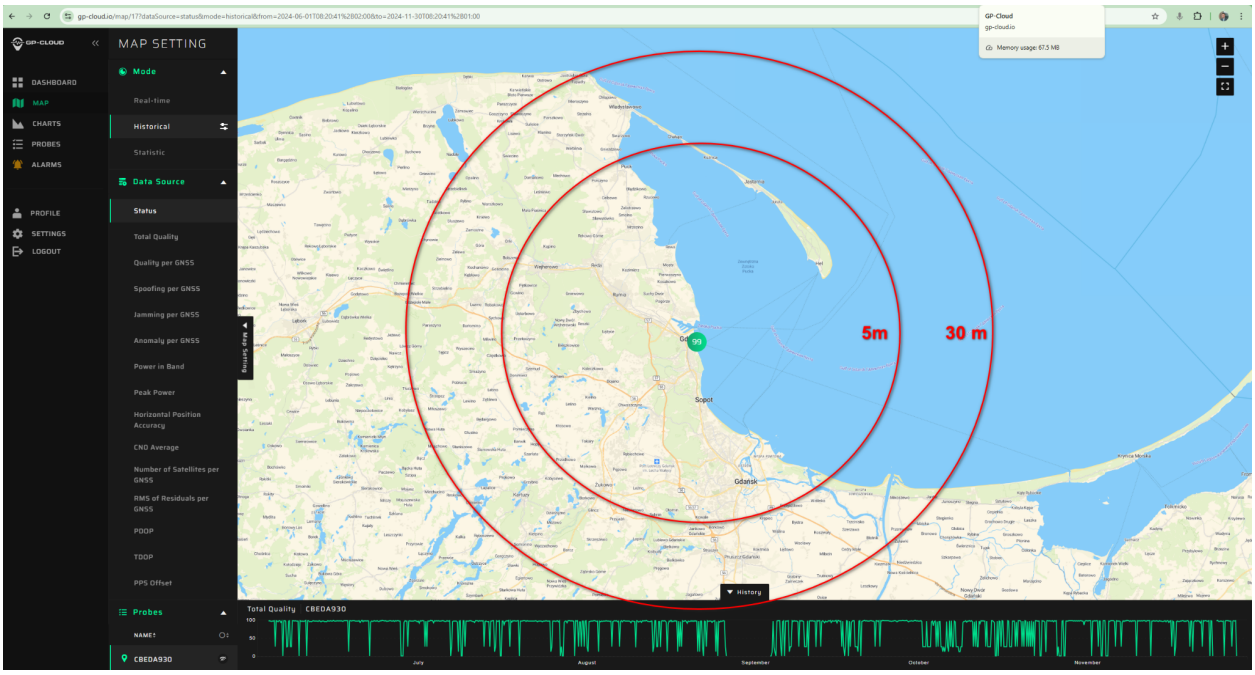
3.1 Sensor Deployment Location

The GP-Probe TGE2 sensor was installed on the third floor of the Faculty of Navigation in Gdynia, situated directly on the Baltic Sea coast. The minimum distance from the installation site to the border with Kaliningrad is approximately 70 km:

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

The height of the sensor's receiving antennas were approximately 15 meters above sea level. Given that a potential interference source's transmitting antenna could be located at a similar height, the estimated **radio horizon** would be **32 km**. The diagram below illustrates the estimated detection range for an interference source with transmitting antennas positioned at different heights (5 m, and 30 m) at sea level:



The corresponding radio horizon distances for each case are presented in the table below:

Probe's Antennas Height, M	Interference Source Antenna Height, m	Max Detection Range, km
15	1	20.08
15	3	23.09
15	5	25.17
15	15	31.91
15	30	38.52
15	50	45.09
15	100	57.16

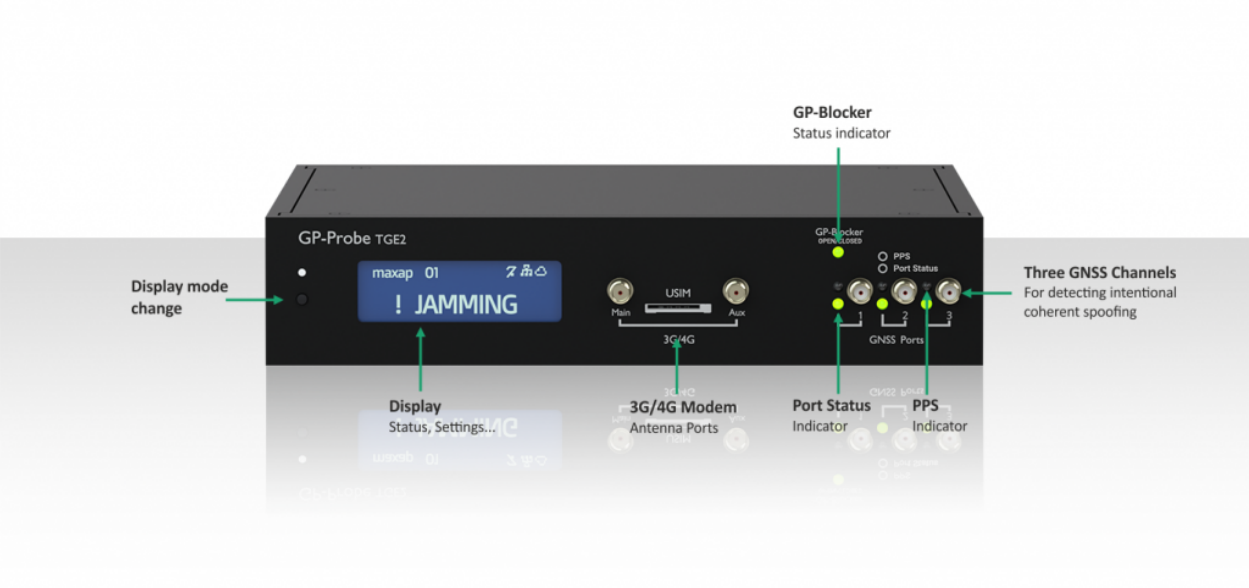
© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

3.2 GNSS Interference Detector

GNSS Interference Detector: GP-Probe TGE2 - CH3 4G RFSA

The GP-Probe TGE2 is a three-channel GNSS interference detection probe equipped with an integrated RF signal analyzer. It was deployed to continuously monitor GNSS signal quality and detect interference events in real time. The device was connected to the GP-Cloud platform via a 4G cellular network.

Traceable GNSS: **GPS L1, Galileo E1, GLONASS G1.**



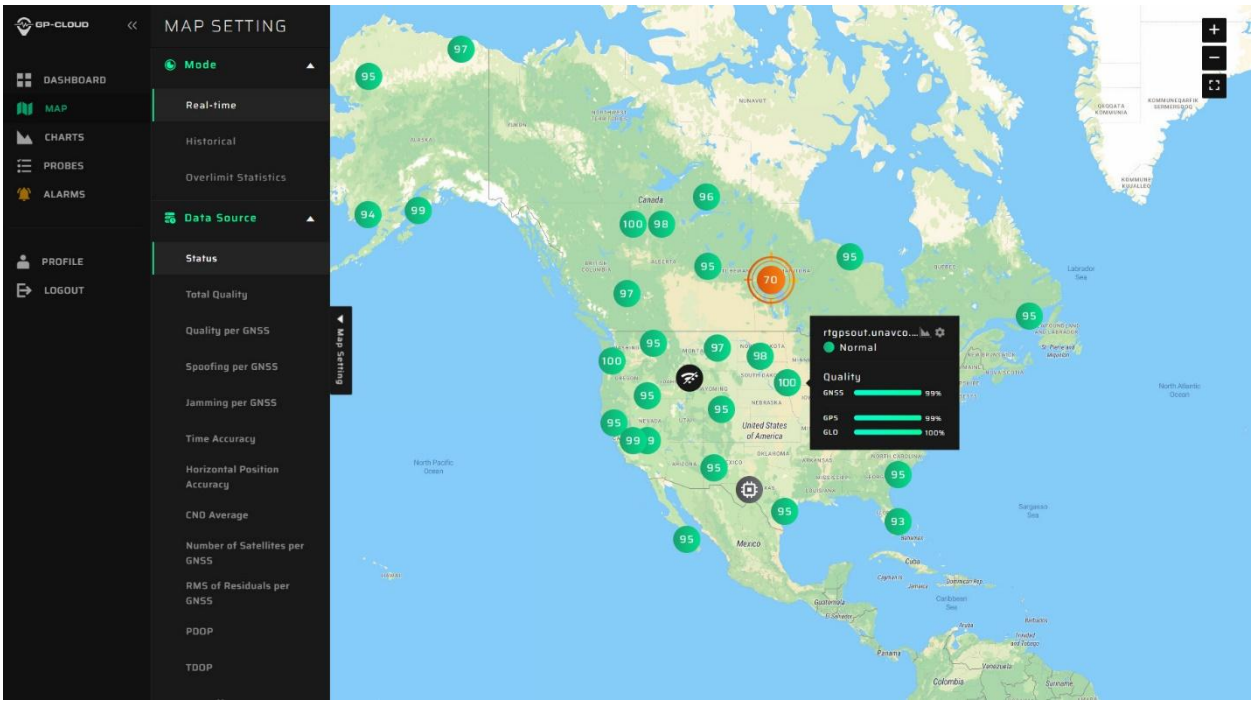
Technical Specifications:

- Three GNSS channels enable spatial signal analysis, ensuring reliable detection of a sophisticated coherent GNSS spoofing scenarios
- GNSS signal quality analysis
- The built-in 60 MHz RF signal analyzer continuously monitors interference, enabling classification and localization with TDOA (Time Difference of Arrival) techniques
- Form factor: 19-inch rack, half-size.
- Double power module: 110 – 220 AC, 18 – 75 DC.
- PPS input for the external time server health checking.
- 4G modem and 100BASE-TX Ethernet for data transferring to the GP-Cloud.
- Web interface for configuration
- Embedded LUA scripting language to create a custom scenario

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

3.3 GP-Cloud: GNSS Signal Quality Monitoring and Analysis

GP-Cloud is the heart of the GPSPATRON system, responsible for processing and analyzing data coming from the connected detector in real time. It offers advanced tools for detecting and assessing GNSS jamming and spoofing.



Key Features:

- Real-time Detection: GP-Cloud processes raw data from connected GP-Probes, analyzing GNSS signal quality and accuracy to detect any anomalies such as spoofing or jamming.
- Data Logging and Reporting: GP-Cloud logs all detected events, providing historical data for post-event analysis. It can generate detailed reports and real-time statistics on system performance and detected threats.
- Scalable Architecture: The cloud platform supports limitless horizontal scaling, making it suitable for large-scale deployments.
- Integration: It supports various GNSS data protocols such as RTCM, NMEA, and Septentrio SBF, and can be integrated with external systems via its REST API.
- Interface: Offers a user-friendly web interface with dashboards, maps, and spectrograms for real-time monitoring and event visualization.

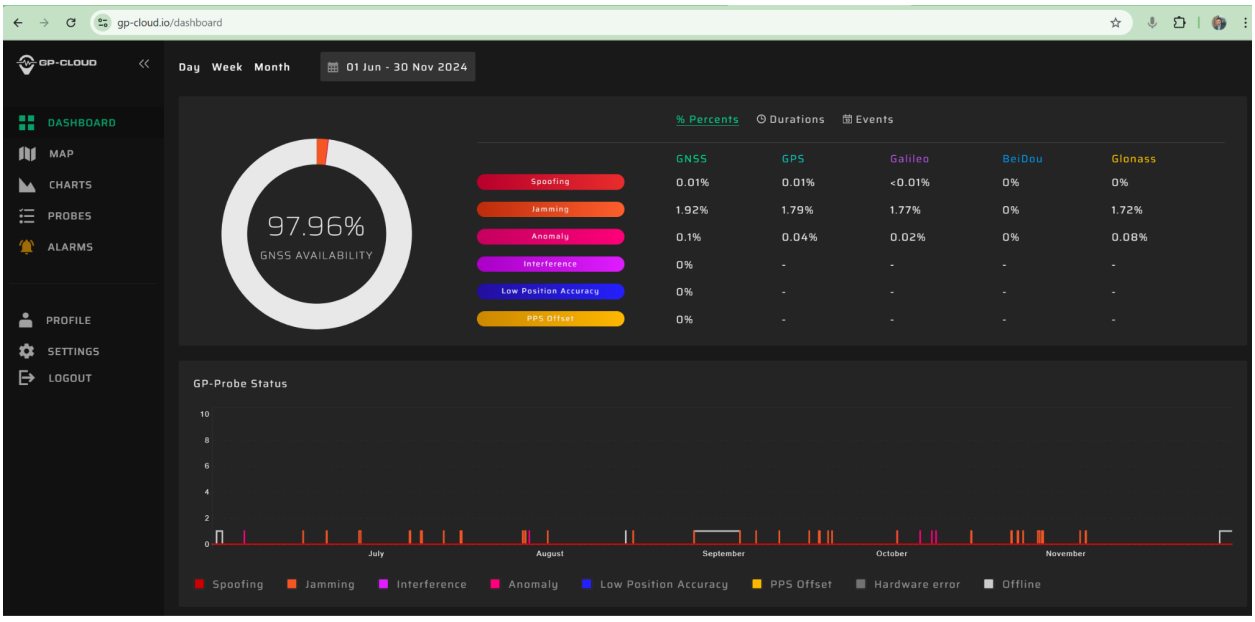
© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

4. GNSS Interference Detection Statistics

In this section, we present the results of GNSS interference monitoring based on six months of collected data, from June to the end of November. The following statistics were derived from GP-Cloud, where all interference detection events were logged and analyzed.

4.1 Summary of Six-Month Interference Data

The GP-Cloud dashboard provides a visual summary of GNSS interference activity over the six-month observation period. The first screenshot presents the distribution of detected interference events in percentage form, showing how spoofing, jamming, and anomalies contributed to the total monitoring time.



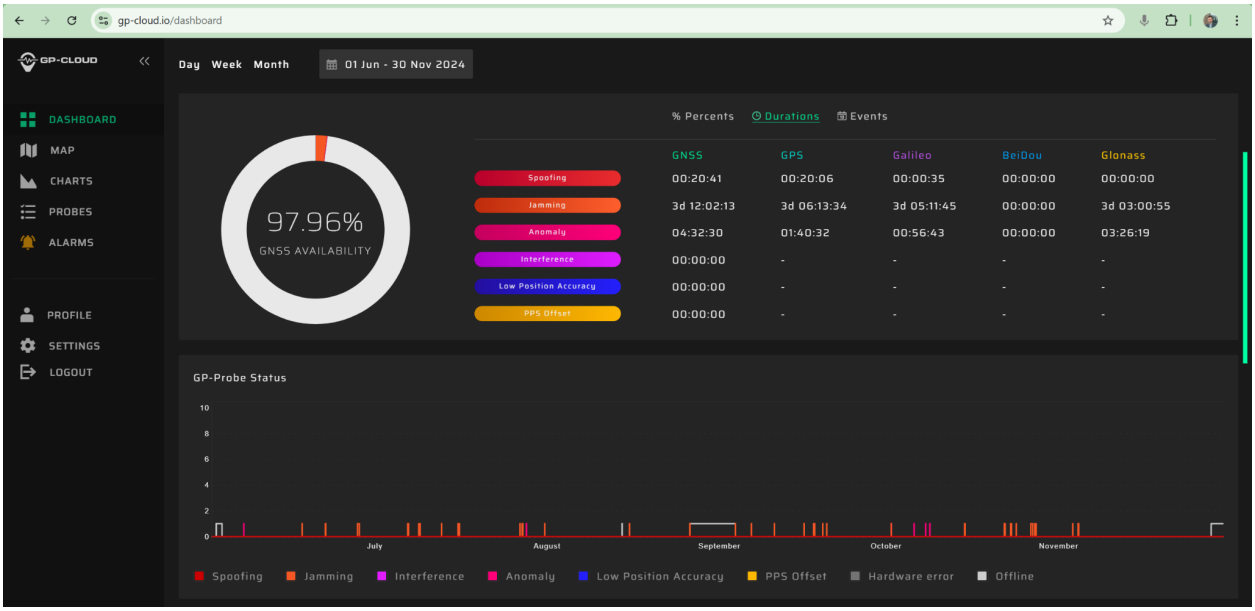
Over the six-month observation period, GNSS signals remained available with the required quality for **97.96% of the time**, meaning that only **2.04% of the collected data** was affected by interference, data anomaly or signal quality degradation.

The breakdown of detected interference is as follows:

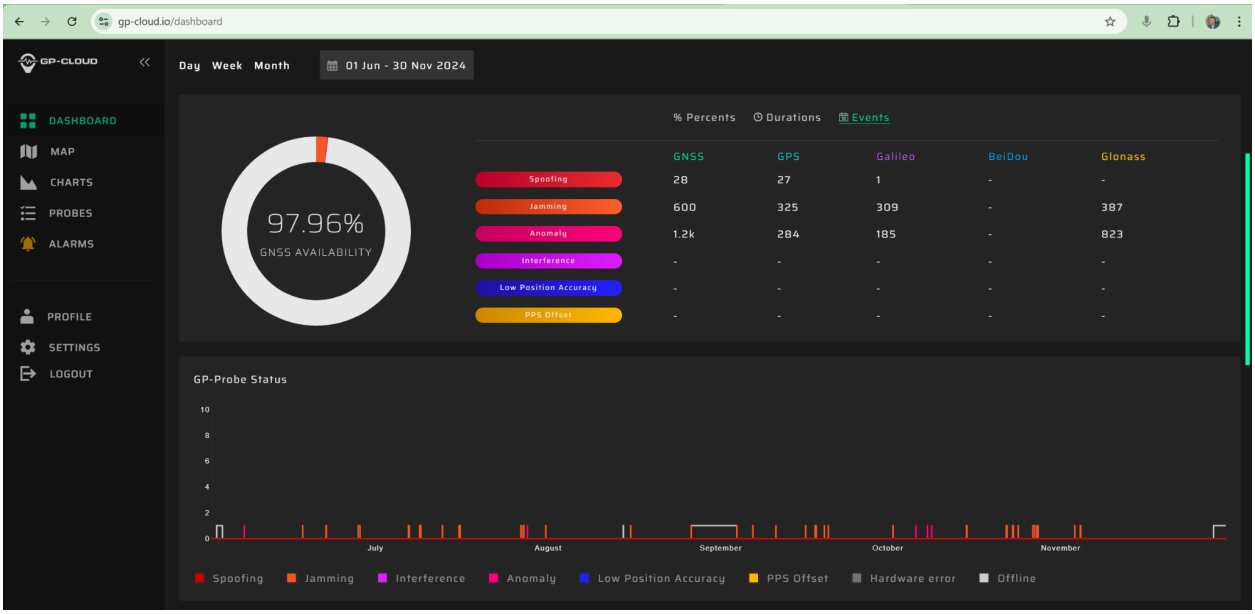
- **Jamming:** Detected in **1.92% of the total monitoring time**, with interference distributed across **GPS, Galileo, and GLONASS constellations** approximately evenly.
- **Spoofing:** Identified in **0.01% of the total monitoring time**, exclusively affecting **GPS signals**.
- **Data anomalies:** Accounted for **0.1% of the total monitoring time**, representing signal inconsistencies that could not be classified as either jamming or spoofing.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

The second screenshot displays the cumulative duration of interference incidents, offering a clear representation of how long each type of disruption persisted over traceable constellations.



The third screenshot focuses on the total number of detected events:



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Analysis of the six-month GNSS interference data from GP-Cloud reveals key trends in spoofing, jamming, and anomaly detection.

- **Spoofing:** A total of 26 spoofing events were detected, accumulating to **20 minutes** of spoofing activity. Given the low duration and scattered occurrences, these detections are likely **false positives**, resulting in a false detection rate below 0.01%. This is a good result for a system operating in real time under actual environmental conditions rather than a controlled laboratory setting.
- **Jamming:** In contrast, GNSS jamming was significantly more persistent, with an overall duration of **84 hours (3 days and 12 hours**). Jamming incidents were evenly spread across different GNSS constellations, confirming a widespread presence of interference throughout the monitoring period.
- **Anomalies:** The system logged 4 hours and 32 minutes of anomalies, detected directly via GNSS observations from the built-in receivers within the sensor. These anomalies indicate unusual disruptions in received signals that could not be definitively classified as either jamming or spoofing.

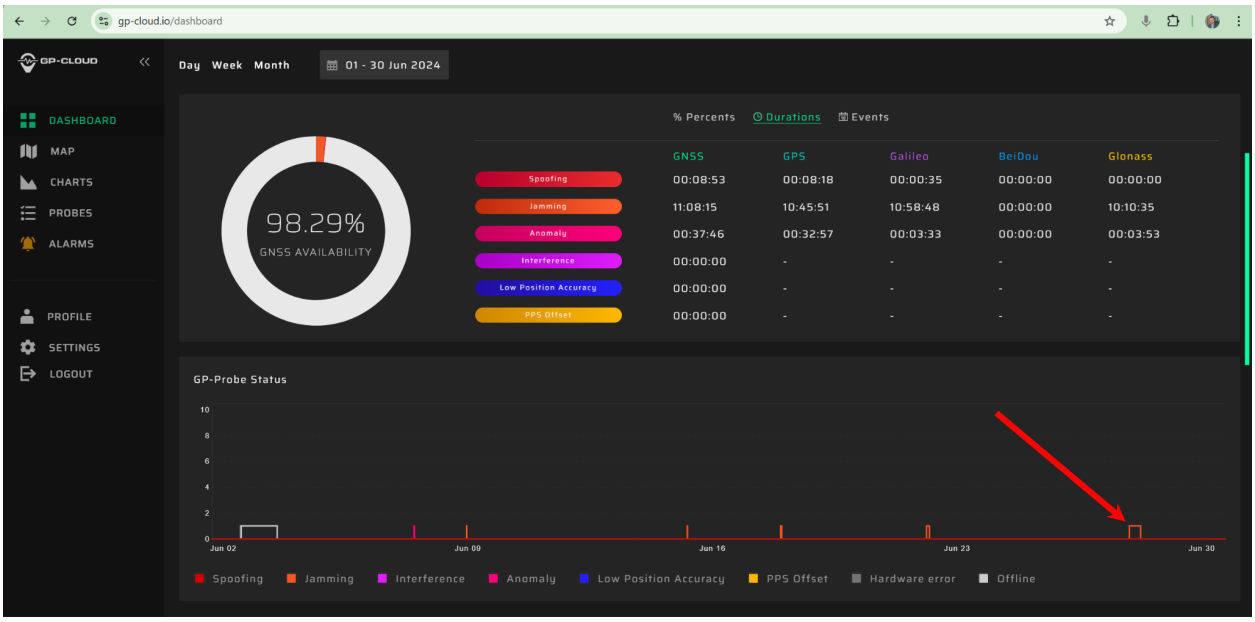
The statistical breakdown highlights how GNSS jamming remains the dominant interference type in the region, while spoofing detections are minimal and likely misclassified events. The presence of anomalies suggests that some interference cases may exhibit complex characteristics, requiring further investigation.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

4.2 Monthly Breakdown of Interference Events

June: Isolated but Prolonged Incident

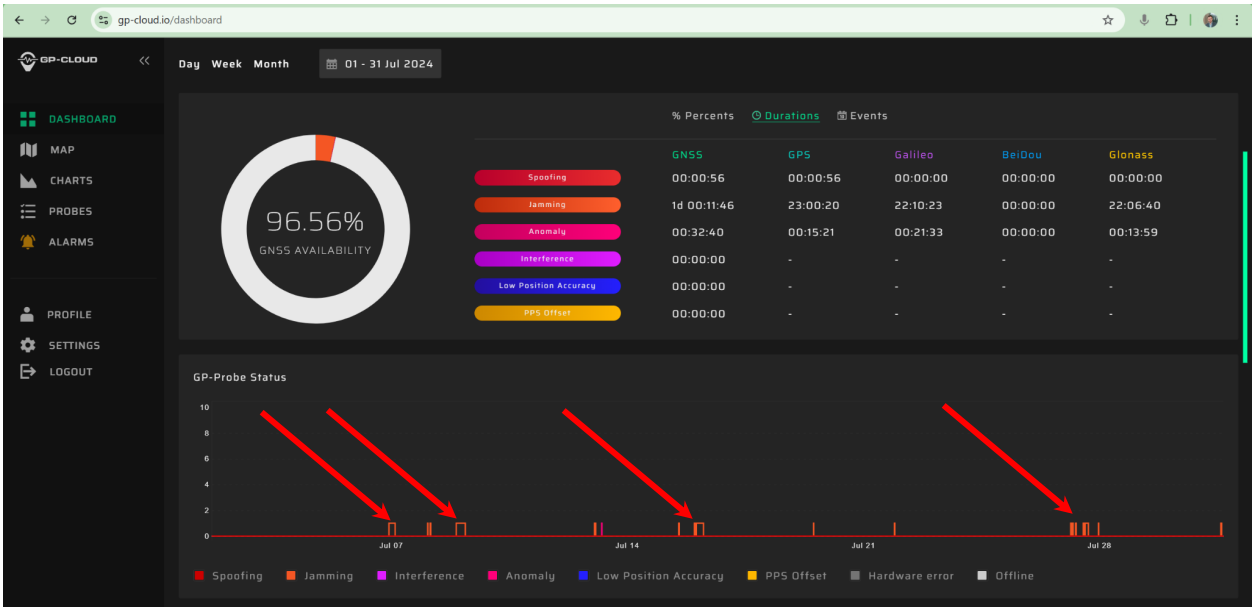
- **Total jamming duration:** 11 hours
- **Number of major incidents:** 1
- **Observation:** A single prolonged jamming event occurred overnight from **June 27 to June 28**, accounting for nearly all the interference detected in this month.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

July: Increased Frequency and Duration

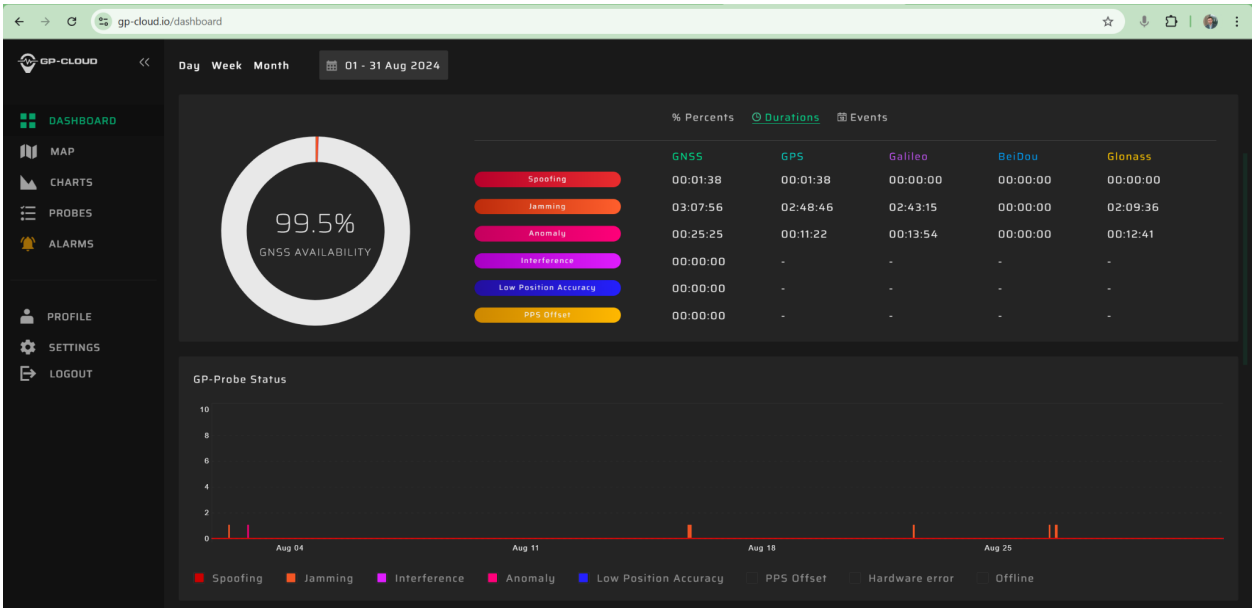
- **Total jamming duration:** 24 hours
- **Number of major incidents:** 4
- **Observation:** Jamming activity significantly increased compared to June, with **four prolonged interference episodes** occurring throughout the month.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

August: Minimal Interference Activity

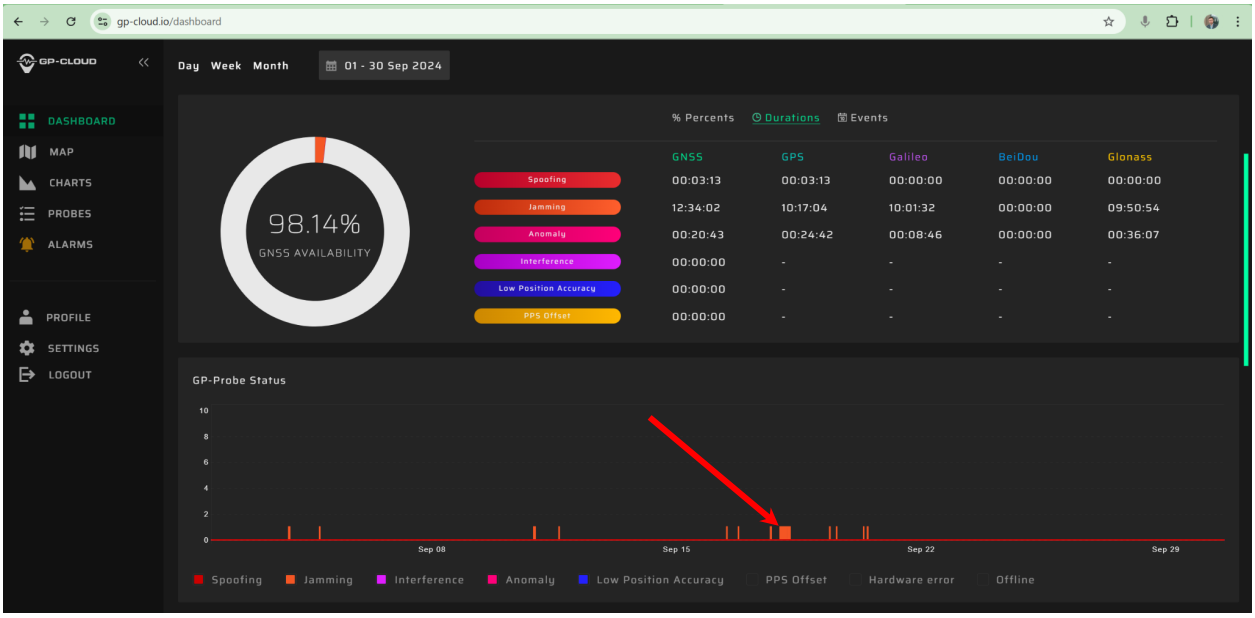
- **Total jamming duration:** 3 hours
- **Number of incidents:** Multiple short-duration events
- **Observation:** Jamming incidents were sporadic and of short duration.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

September: A Single Major Incident

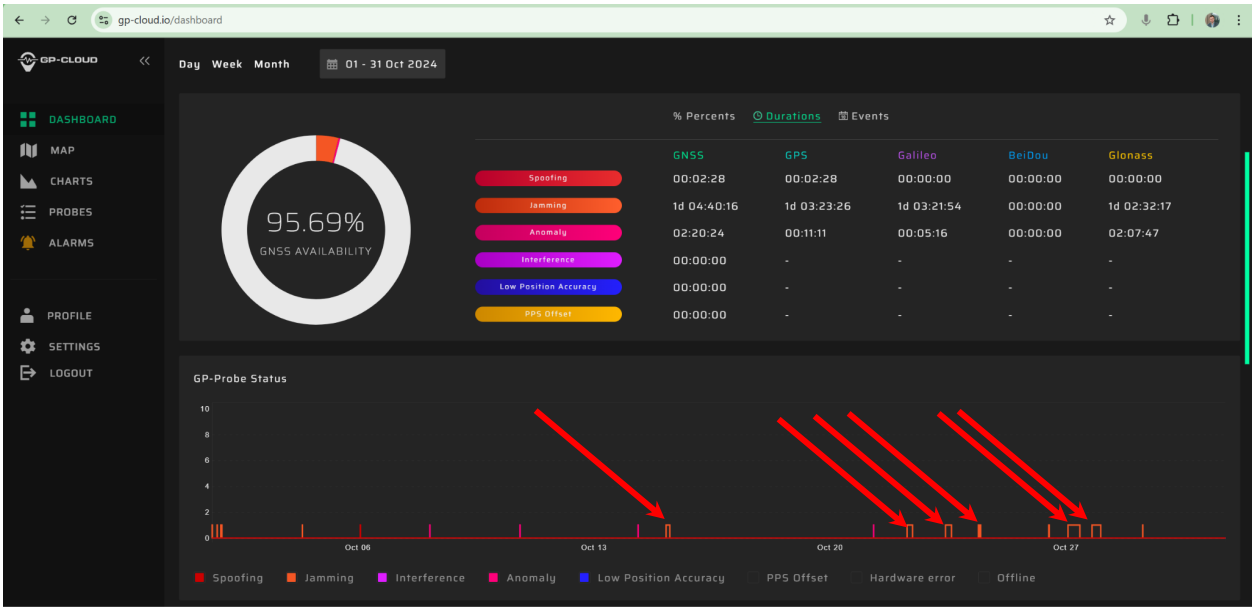
- **Total jamming duration:** 12 hours 34 minutes
- **Number of incidents:** 1 major event
- **Observation:** Most interference was attributed to a **single prolonged jamming event overnight from September 17 to September 18**.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

October: Peak Jamming Activity

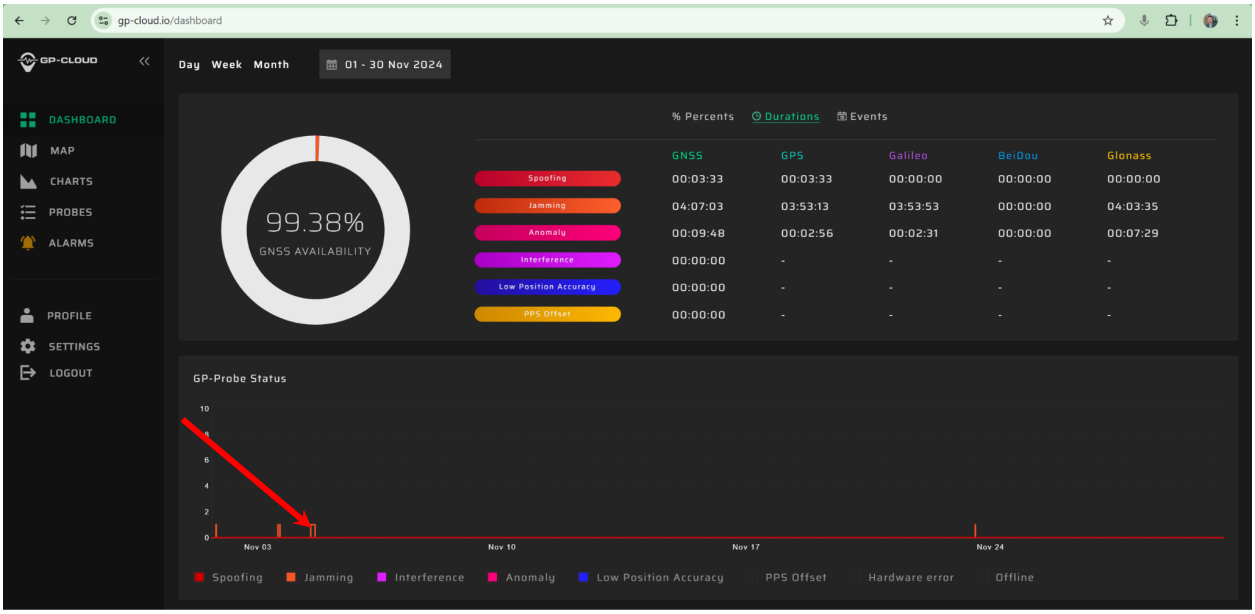
- **Total jamming duration:** 29 hours
- **Number of incidents:** 6
- **Observation:** October recorded the highest level of jamming activity, with **six separate incidents**, suggesting a significant rise in GNSS disruptions.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

November: Isolated Yet Notable Interference

- **Total jamming duration:** 4 hours
- **Number of incidents:** 1 major event
- **Observation:** Most of the interference in November was concentrated in a **single relatively short-duration event on November 4**.

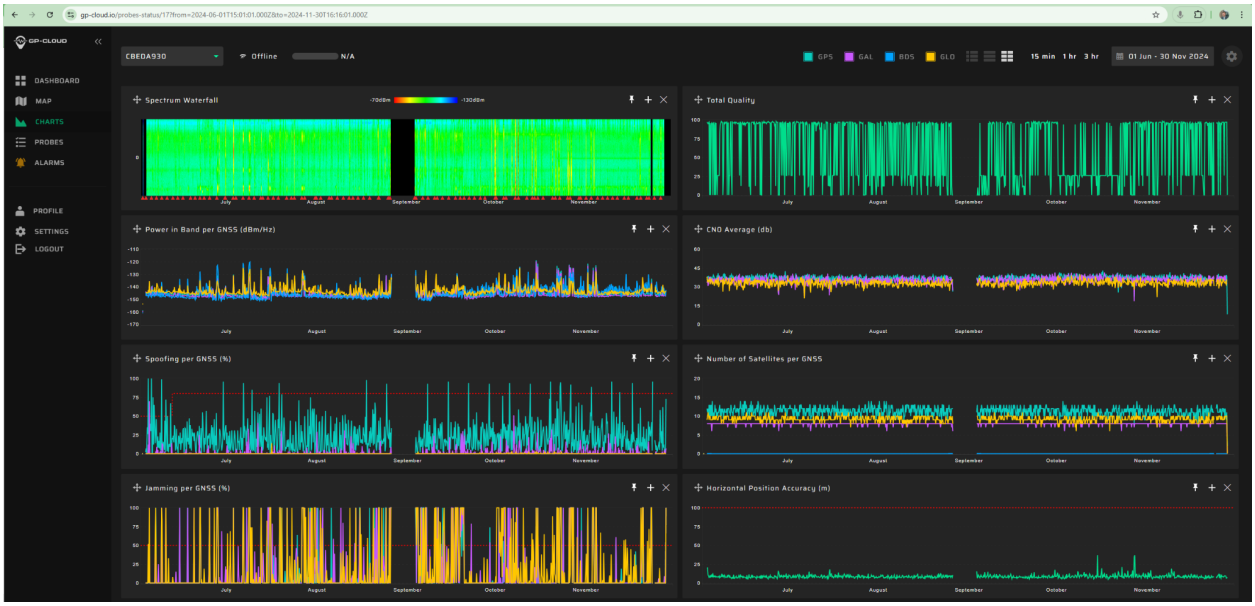


© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5. Detailed Analysis of Interference

To analyze detected GNSS interference events, the system provides a set of visualization tools integrated into the cloud platform's user interface. These tools enable post-event examination of interference characteristics using recorded spectrum information and GNSS observation.

The screenshot below presents data from six months of observations. Strong interference events are clearly visible on the spectrum waterfall and power level graph:



Each detected event can be reviewed through multiple analytical graphs and metrics:

- **Spectrum Waterfall Plot:** Displays the frequency-time distribution of interference, with color intensity representing signal power. This helps identify the duration, bandwidth, and variability of interference signals.
- **Power Level Graphs:** Show variations in signal power over time for each GNSS constellation, highlighting the impact of interference on different bands.
- **Jamming and Spoofing Detection Probability:** Provides confidence levels for interference classification, indicating how certain the system was in identifying an event as jamming or spoofing.
- **GNSS Signal Quality Metrics:** Assesses overall signal reception conditions under interference.
- **Average Signal-to-Noise Ratio (SNR):** Displays **SNR degradation** under interference, showing drops in SNR during jamming periods.
- **Number of Visible Satellites:** Plots satellite visibility variations for each constellation, revealing signal loss trends under jamming conditions.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

- **Positioning Accuracy Graph:** Demonstrates how interference affected positioning accuracy, with observed degradation from a baseline of ~7 meters to ~40 meters under strong interference.

By analyzing these visualized parameters, interference events can be categorized based on their characteristics, duration, and severity. This structured approach allows for an in-depth understanding of GNSS signal disruptions and their potential impact on ground-based navigation and timing applications.

5.1 Interference Event on June 27–28

A significant GNSS interference event was recorded between **22:25:42 CET on June 27** and **06:09:35 CET on June 28**, lasting for **7 hours, 43 minutes, and 53 seconds**.

Signal Characteristics and Source Hypothesis

The interference event exhibited noticeable fluctuations in power levels, suggesting that the jamming source was in motion. Given the system's radio horizon, which primarily covers a portion of the Baltic Sea, and assuming that the interference source was not located within Poland's borders, the most plausible explanation is that the jamming originated from a vessel in international waters.

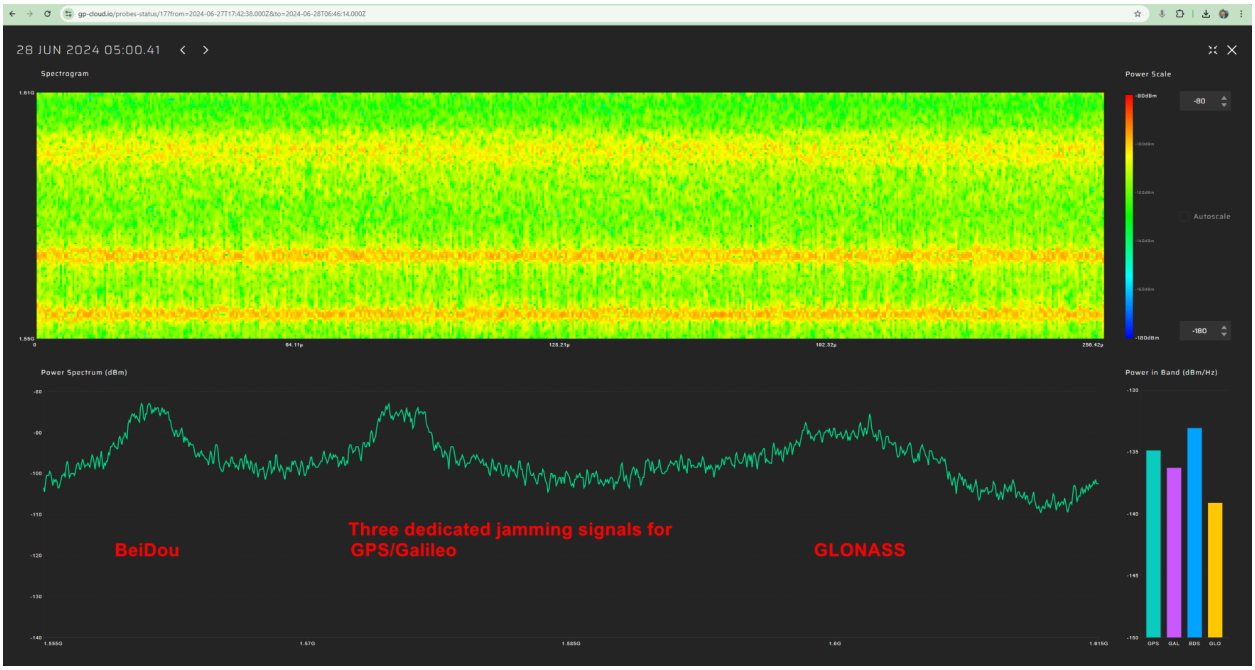
The detected interference signal exhibited relatively low power, leading to only minor degradation in the **signal-to-noise ratio (SNR) for GPS, Galileo, and GLONASS**. Despite this, the system classified the event as **100% jamming across all tracked constellations**, with no spoofing signatures detected.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Impact on GNSS Performance

- **Positioning Accuracy:** No significant degradation in positioning accuracy was observed during the interference event.
- **Signal-to-Noise Ratio:** Minor degradation was detected across GPS, Galileo, and GLONASS signals, but not severe enough to disrupt positioning or tracking performance.

Spectral Analysis and Jamming Structure



Spectrogram analysis revealed that the jamming signal had a complex structure, consisting of **three distinct interference components** targeting:

1. **BeiDou**,
2. **GPS and Galileo**,
3. **GLONASS**.

This structured interference pattern indicates the use of **sophisticated and purpose-built jamming equipment**, capable of selectively targeting multiple GNSS constellations. The deliberate nature of the interference, along with its multi-constellation targeting, strongly suggests that this was an **intentional jamming operation** rather than incidental RF noise or unintentional interference.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.2 GNSS Interference Events in July

All detected GNSS interference events in July have been grouped into a single section, as their spectral characteristics and modulation patterns indicate a common origin. The interference signals share the same structure across all recorded events, suggesting that they were likely emitted by the same source, most probably a vessel operating in the Baltic Sea.

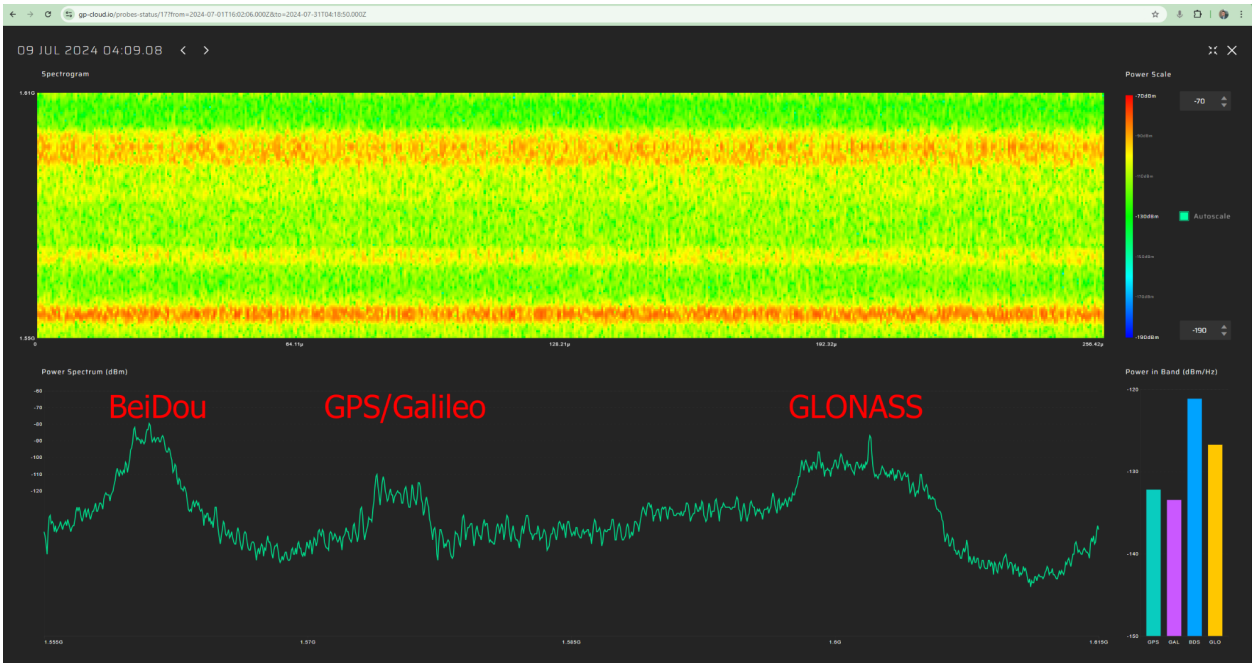
Four major interference events were recorded in July, each exhibiting the same modulation pattern:

Event	Start Time (CET)	End Time (CET)	Duration
1	July 6, 22:34	July 7, 03:04	4 hours 30 minutes
2	July 8, 22:25	July 9, 04:52	6 hours 27 minutes
3	July 15, 23:33	July 16, 06:22	6 hours 49 minutes
4	July 27, 03:11	July 27, 23:37	20 hours 26 minutes (intermittent)

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Interference Characteristics

- **Spectral Analysis:** All major interference episodes displayed an identical modulation type, reinforcing the hypothesis of a single, recurring interference source.



- **Possible Source:** Given the system's radio horizon limitations and the absence of domestic interference sources within Poland, the most likely origin remains a vessel in international waters.
- **Operational Pattern:** The interference events consistently occurred during nighttime and early morning hours, which may indicate a specific operational schedule of the jamming source.
- **Signal Strength and Impact:** These events exhibited relatively **high power levels**, leading to a **significant decrease in the signal-to-noise ratio (SNR)** for GPS, Galileo, and GLONASS. This degradation suggests that the interference was strong enough to notably affect GNSS reception, potentially reducing positioning accuracy and reliability in the affected area.

The spectrogram below provides a month-long visualization of detected interference, illustrating the repeated and structured nature of the events.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.3 Interference Events on July 6–7 and July 8–9

Interference Event on July 6–7

The first significant interference event in July began on **July 6 at 22:34 CET** and gradually decreased in power until it became completely undetectable by **03:04 CET on July 7**. The smooth and continuous decline in power suggests that the interference source was in motion throughout the event. Given the system's limited radio horizon, the most plausible explanation is that the interference originated from a vessel moving away from the monitoring station. The gradual decrease in interference power over several hours is consistent with a slow-moving maritime object exiting the detection range.

Interference Event on July 8–9

The second major interference event was activated on **July 8 at 22:25 CET** and remained active until **04:52 CET on July 9**. Unlike the event on July 6, this interference exhibited **significant power fluctuations**, suggesting that the source was either stationary or moving within a limited area. The lack of a consistent power decrease over time indicates that the interference source was not steadily moving away but rather fluctuating in position, possibly within a small operational zone.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Analysis of Power Variations and Source Behavior

- Both interference events started with similar power levels, suggesting that the jamming source was initially at a comparable distance from the sensor in both cases.
- The **July 6–7 interference** showed a gradual and continuous decline, which strongly indicates that the source was moving away from the monitoring site, likely a vessel leaving the area.
- The **July 8–9 interference** exhibited strong fluctuations in power but no clear directional movement. This pattern suggests that the source was either **stationary or moving within a confined area**.
- The abrupt activation of both interference events suggests that the crew of the transmitting vessel enabled the jammer, potentially in response to a specific operational need. While the exact motivation remains unknown, the repeated activation of strong jamming signals could indicate an attempt to **conceal certain activities** that might not comply with legal regulations.

Classification and Impact on GNSS Signals

- Both interference events were classified as **GNSS jamming**, with no strong spoofing signatures detected.
- The **interference power was strong enough to cause a clear degradation in the signal-to-noise ratio (SNR)** for GPS, Galileo, and GLONASS signals, although no significant degradation in positioning accuracy was observed.
- Between the two major interference events, **a weaker signal with the same modulation pattern was briefly visible for several hours**.

These findings reinforce the hypothesis that the interference originated from a vessel operating within the Baltic Sea, with its movement influencing the power variations detected by the monitoring system.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.4 Unusual Interference Pattern on July 27

An anomalous interference event was detected on **July 27 at 03:11 CET** and persisted until **23:37 CET**. Unlike previous incidents, this interference was **intermittent**, appearing and disappearing multiple times throughout the observed period.

Interference Characteristics

- The interference exhibited **fluctuating power levels**, with some instances reaching sufficiently high levels to **significantly degrade GNSS signal reception**.
- All detected interference instances were classified as **jamming**, with **no spoofing signatures** identified.
- The **power graph suggests that the interference was not activated instantaneously** but rather behaved as if the source was **rapidly approaching, remaining in position, and then abruptly moving away**.

The cause of this unusual behavior is difficult to determine without additional data. The pattern could suggest:

1. **A moving platform periodically entering and exiting the detection range**, potentially a vessel maneuvering within a specific area.
2. **A variable power jamming system**, either intentionally modulating its transmission or experiencing environmental factors affecting its signal propagation.

Due to the inconsistent activation pattern and abrupt power fluctuations, the **exact nature and intent of this interference remain unclear**.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.5 GNSS Interference Events in August

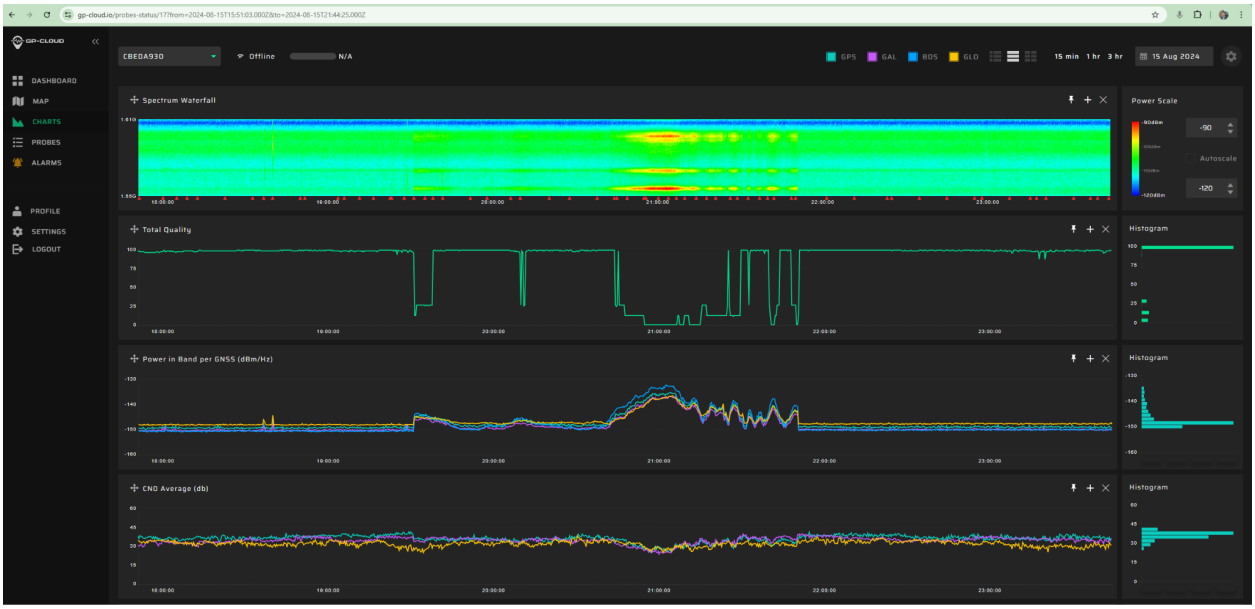
August showed a **significant decrease in interference activity**, likely due to seasonal factors. No major jamming incidents were detected during the month. The screenshot below presents an overview of all interference events recorded throughout August.

Repeated Interference Pattern from June and July

A single interference event matching the **same modulation type** as those observed in June and July was detected on **August 15 from 19:30 to 21:50 CET**. The interference gradually increased

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

and then faded away, but its power remained **relatively low** throughout the event.



Detection of Unusual Modulation Types

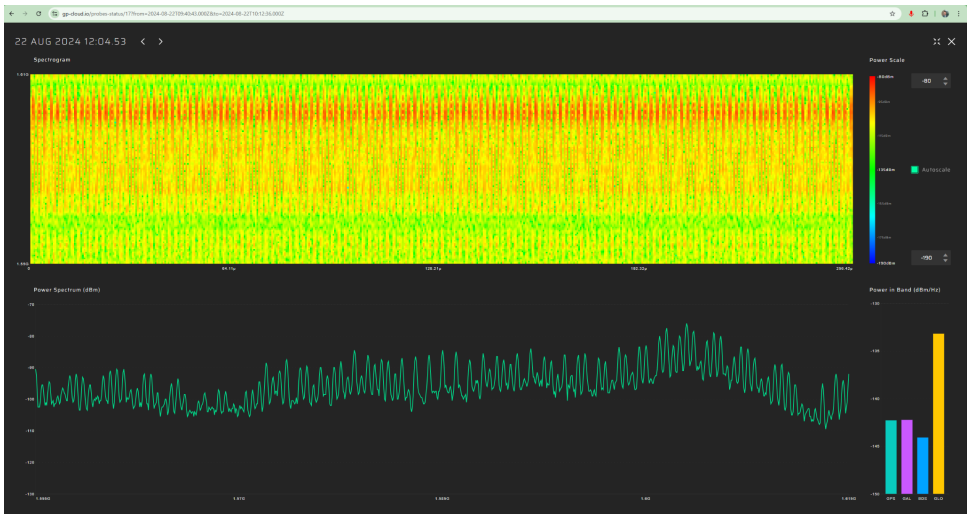
Although strong jamming signals were mostly absent, the system detected **two interference events with unique modulation characteristics**, which are of particular interest:

1. **Pulsed Frequency-Modulated Interference (August 22, 11:46 – 12:06 CET)**

- This interference had a **high-power pulsed nature**, repeatedly turning on and off.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

- Each activation lasted only a **few tens of seconds**, but during these periods, it **severely degraded GNSS reception quality**.
- Spectrogram analysis shows that the signal was **frequency modulated with an extremely short sweep period of approximately 2 microseconds**, which could indicate the use of **a high-end jamming system**.



2. **Multi-tone Modulation (August 26)**

On August 26, a high-power interference event was detected, exhibiting a well-defined multi-tone signal structure. Unlike typical GNSS jamming waveforms, multi-tone signals are not commonly used for intentional GNSS disruption, making it difficult to determine the exact nature of the equipment responsible for this interference.

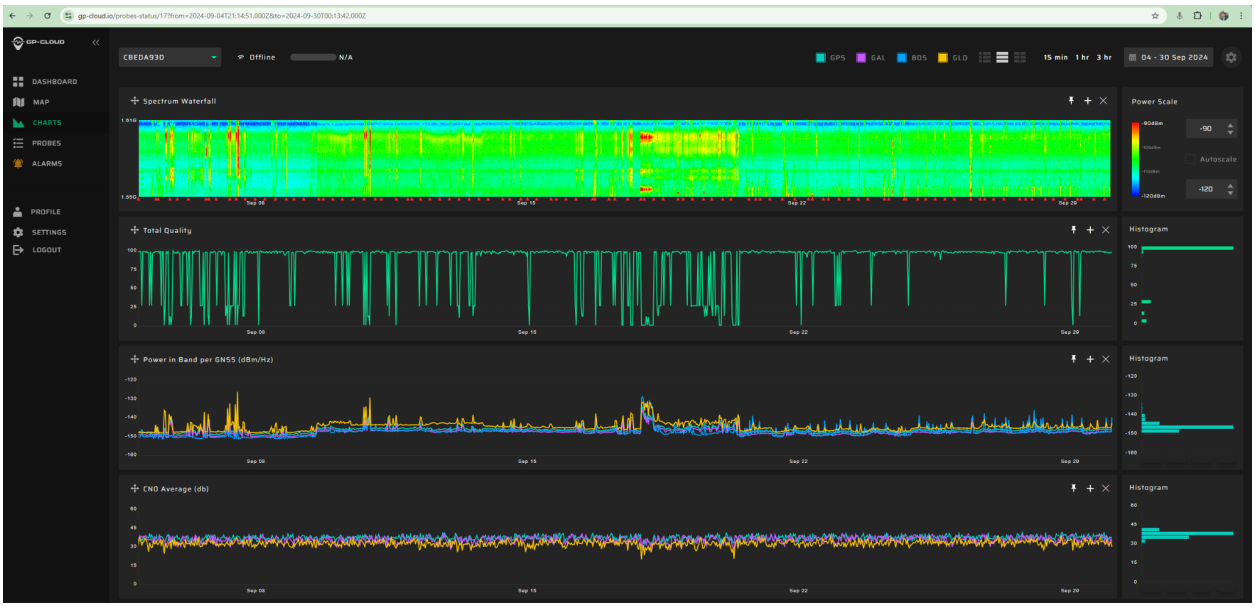
© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

A notable characteristic of this event was **significant fluctuations in the central frequency**, observed throughout the duration of the signal. This behavior suggests that the interference might not originate from a conventional jamming system but could instead be related to **industrial RF emissions or unintentional interference**. The spectral characteristics of the signal require further analysis to differentiate between **deliberate jamming and potential environmental RF noise**.

5.6 GNSS Interference Events in September

September was characterized by **a large number of short-duration interference events** with **varied modulation types**, predominantly **frequency-modulated signals**. Most of these events did not significantly impact GNSS reception quality, but their diversity in waveform structures makes them noteworthy.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

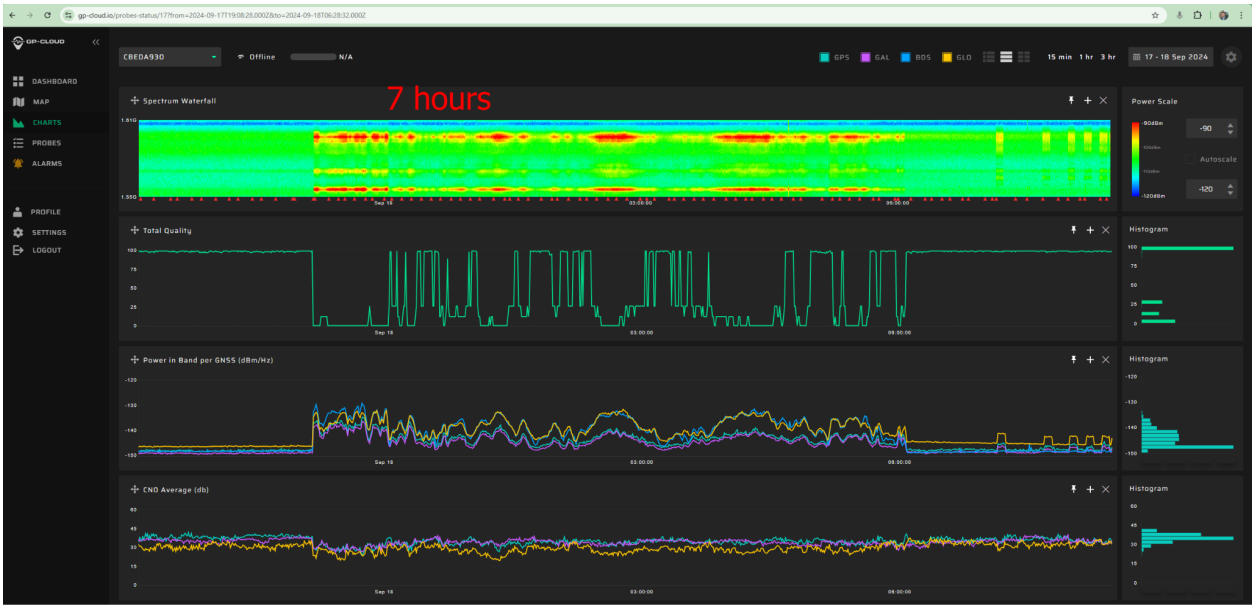


© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

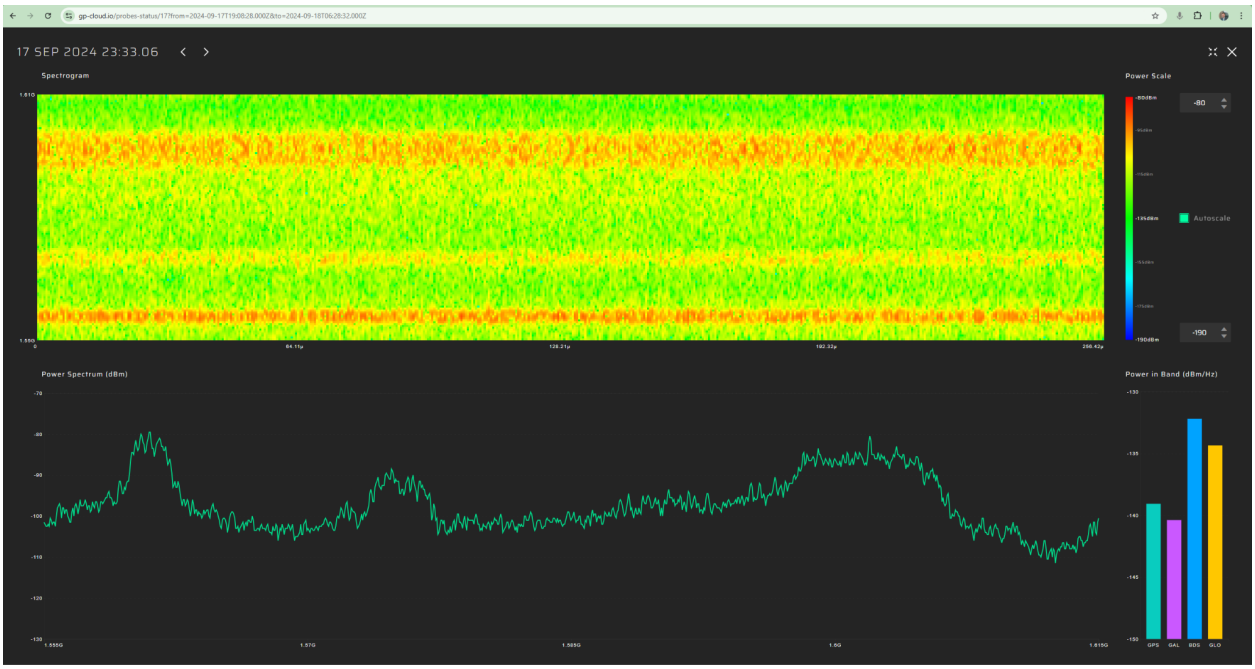
Significant Interference Event on September 17–18

A prolonged interference event was detected on **September 17 at 23:10 CET**, lasting until **September 18 at 06:05 CET**. The interference exhibited **a fluctuating power pattern**, with periods of increased and decreased intensity rather than a steady signal.

Despite the **moderate power levels**, which were not strong enough to cause significant degradation in GNSS reception, the **spectral analysis confirmed that the modulation structure was identical to the interference observed in June and July**. This suggests that the same **type of jamming source** was responsible for this event, although its varying power levels indicate potential changes in transmission conditions or distance from the monitoring station.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.



This was the **only interference event in September that caused a notable degradation in GNSS signal quality**, affecting **signal-to-noise ratios across multiple constellations**.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Analysis of Short-Duration Interference Events

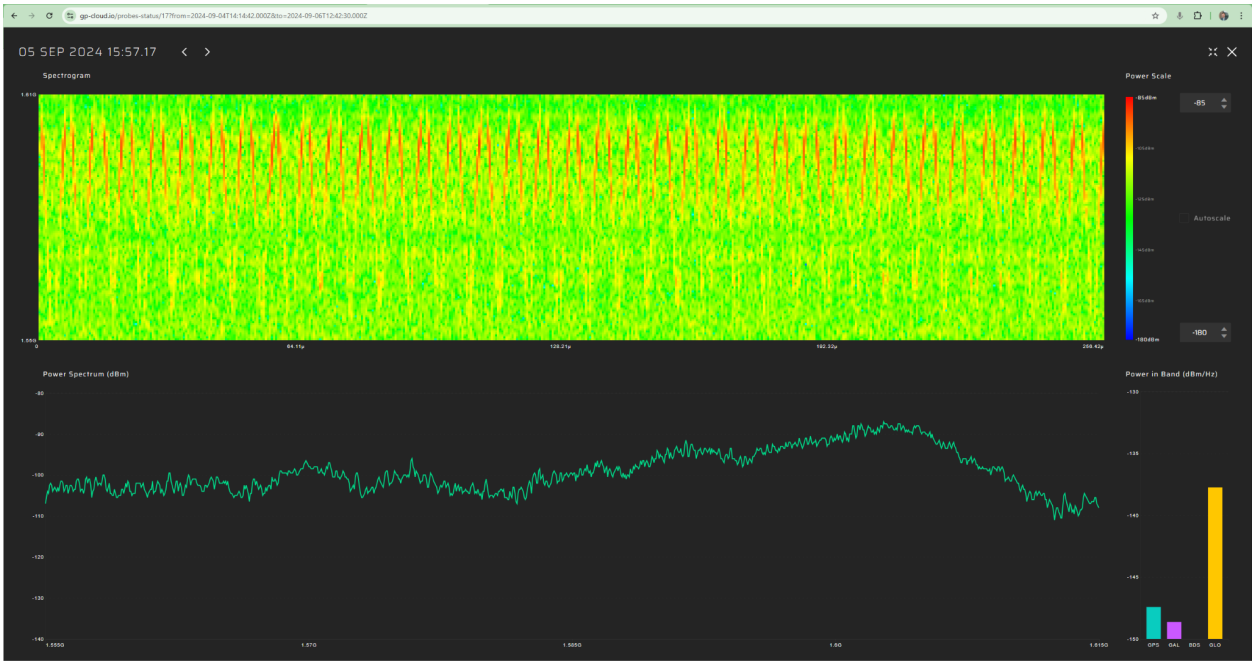
Apart from the major event, multiple **short-duration interferences** with **diverse modulation types** were detected throughout September. These included:

- **Various frequency-modulated waveforms**
- **Different durations and spectral patterns**
- **Minimal impact on GNSS reception quality**

The spectrograms below provide **visual representations of the most interesting interference signals recorded in September**, showcasing their **unique modulation characteristics** despite their limited impact on GNSS performance.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Spectrogram of a frequently observed CHIRP signal in September:



All similar signals detected in September had a very short duration, approximately **10 minutes**, but occurred **frequently throughout the month**.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.7 GNSS Interference Events in October

Short-Duration Industrial Interference in Early October

During the **first half of October**, the interference environment was dominated by **short-duration industrial signals**. These signals were **clearly visible on the spectrum waterfall and power level graphs** but did not have any measurable impact on GNSS signal reception quality. Their characteristics suggest they were likely **unintentional emissions from industrial equipment** rather than deliberate jamming sources.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Multi-Tone Interference Events (October 15–30)

Starting from **October 15**, five **long-duration multi-tone interference events** were detected. These signals were significantly stronger than the earlier industrial interference and persisted for several hours.

Event	Start Time (CET)	End Time (CET)	Duration
1	October 15, 03:30	October 15, 06:05	2 hours 35 minutes
2	October 22, 07:01	October 22, 10:48	3 hours 47 minutes
3	October 23, 10:14	October 23, 14:30	4 hours 16 minutes
4	October 27, 01:24	October 27, 08:51	7 hours 27 minutes
5	October 27, 17:30	October 27, 23:42	6 hours 12 minutes

All these interference episodes featured **a distinct multi-tone modulation**, which was consistently observed in previous months. The **October 15 event** was particularly strong in power, standing out as the most intense among all recorded multi-tone jamming incidents.

5.7.1 Multi-tone Interference on October 15

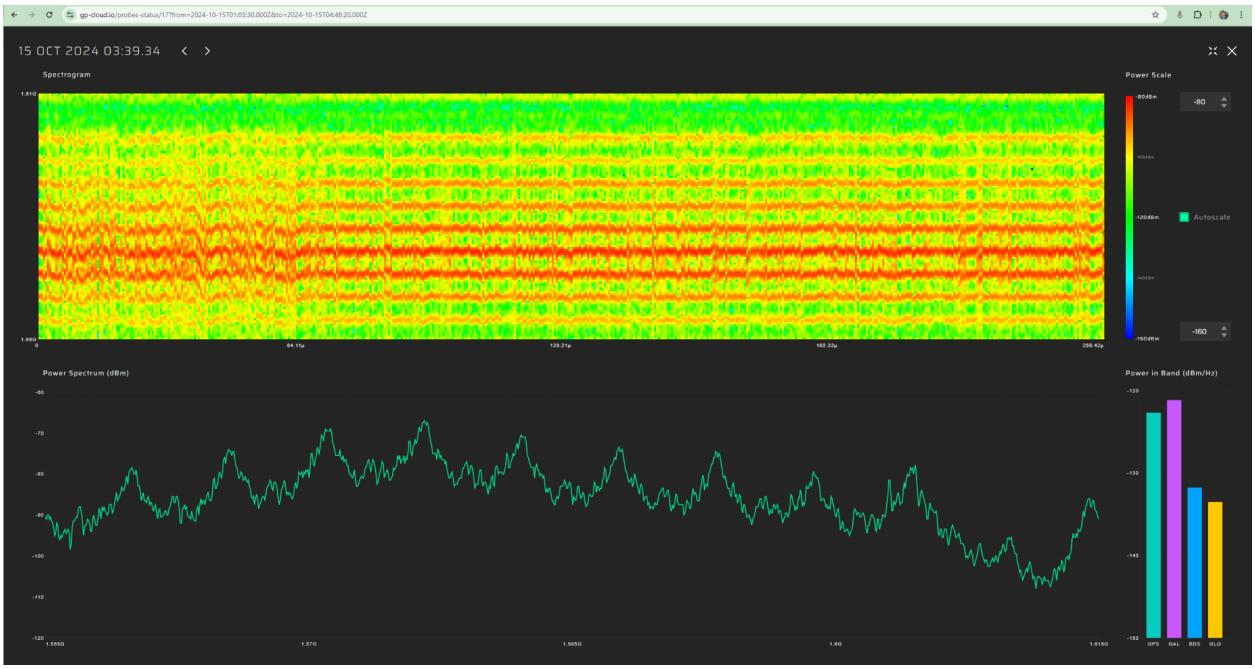
A **strong and well-defined multi-tone interference event** was recorded on **October 15**, starting at **03:30 CET** and ending at **06:05 CET**.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Signal Characteristics

- The interference **maintained a highly stable power level** throughout the event, suggesting that the **source was stationary**.
- The **multi-tone modulation** was clearly visible in the spectrogram, consistent with previously observed jamming signals.



- The system classified this event as **100% jamming across all visible GNSS constellations**, with **no spoofing signatures detected**.

Impact on GNSS Performance

- **Significant SNR degradation** was observed across all monitored GNSS signals.
- **Positioning accuracy degradation** was detected:
  - Under normal conditions, positioning accuracy varied around **3–5 meters**.
  - During the interference event, accuracy degradation was noticeable, occasionally dropping to **36 meters**.

This was one of the few interference events where **a direct impact on positioning accuracy was observed**, indicating that the jamming power was sufficient to disrupt GNSS-based navigation performance rather than just reducing signal quality.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

5.7.2 Multi-tone Interference on October 27

The same multi-tone interference signal detected on October 15 was observed **five times** throughout October. Below is an example of such an event recorded on October 27.

This interference began at 17:30 CET and ended at 23:42 CET, lasting for 6 hours and 12 minutes.

Signal Characteristics

- The interference **exhibited the same multi-tone modulation pattern** as previously observed events.
- The **power level was lower than the October 15 event**, but still sufficient to degrade GPS and Galileo reception quality.

Impact on GNSS Performance

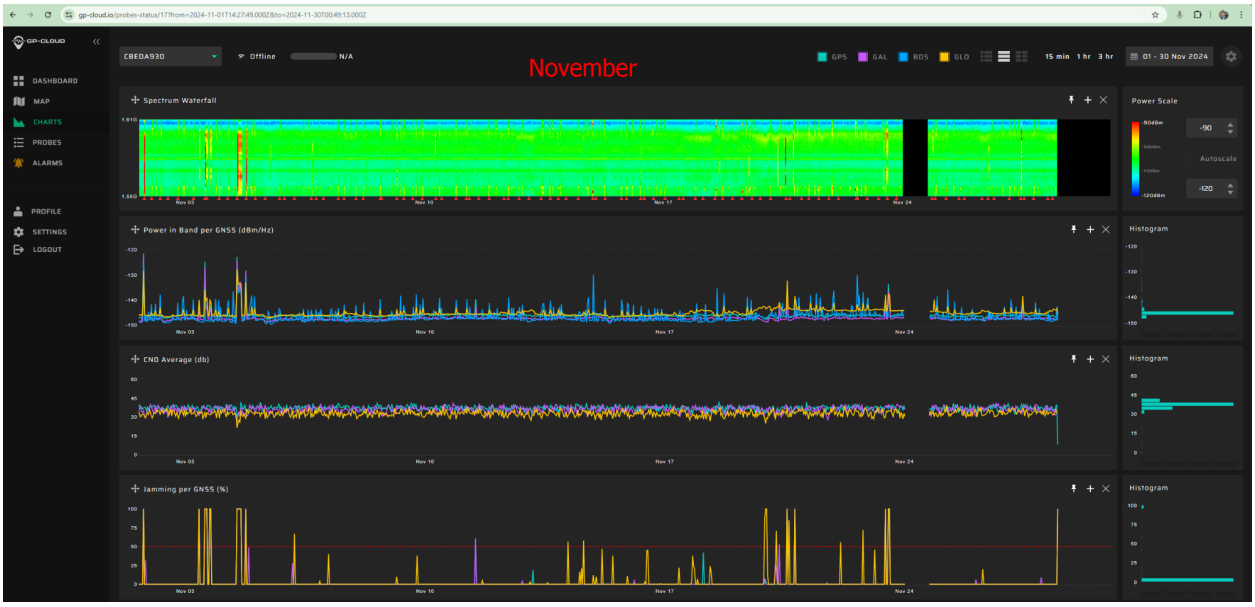
- **GPS and Galileo signals** experienced **significant SNR degradation**, affecting overall signal quality.
- **GLONASS signals** showed **minimal degradation**, likely due to the lower interference power compared to previous high-intensity jamming events.
- **Positioning accuracy was notably affected**, with positioning errors increasing beyond normal levels, similar to the October 15 event.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Despite the lower power compared to earlier jamming incidents, this interference event still had a **measurable impact on GNSS signal reception and positioning accuracy**, reinforcing the need for continuous monitoring of such disruptions.

5.8 GNSS Interference Events in November

November was a **relatively quiet month** in terms of GNSS interference, with only a few notable incidents recorded.



Multi-Tone Interference on November 4

A **single multi-tone interference event** was detected on **November 4 from 12:45 CET to 15:50 CET**. This event followed the same **modulation pattern** as previous multi-tone jamming signals but was isolated and did not repeat throughout the month.

Short-Duration Industrial Interference

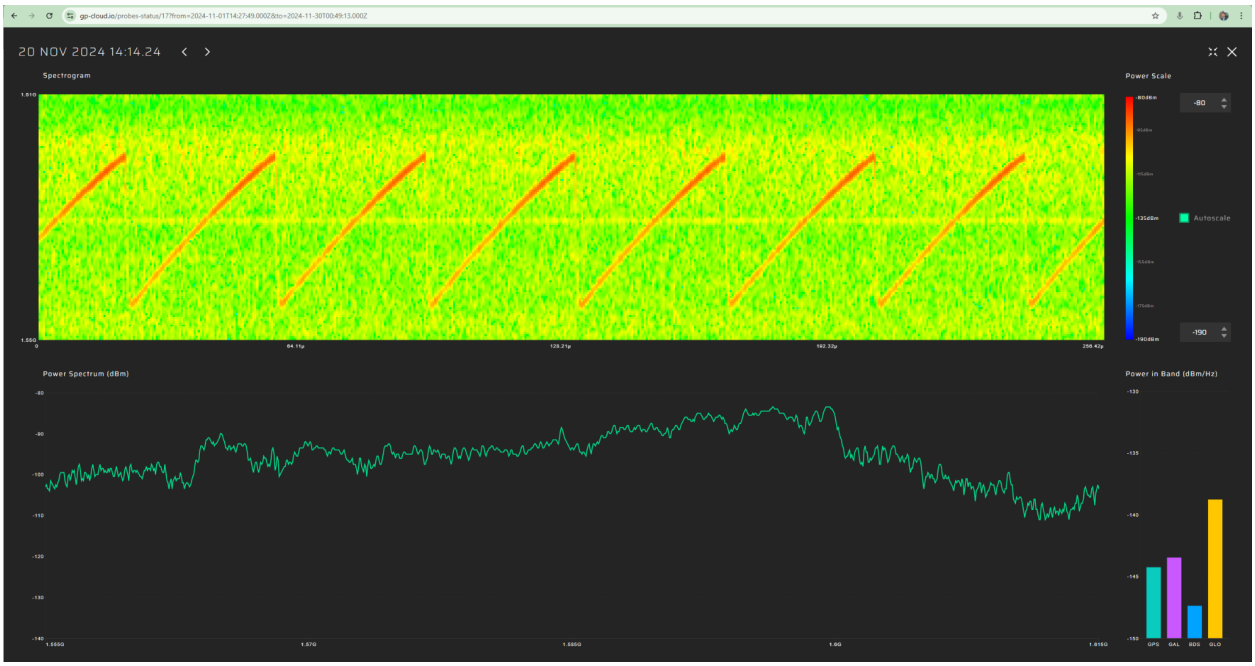
Throughout November, several **short-duration industrial interference signals** were observed. These signals were **brief and did not impact GNSS reception quality**, similar to those detected in early October.

In-Car Jamming

Additionally, multiple cases of automotive jamming were identified, characterized by distinct modulation patterns. These signals closely resembled previously known in-car GNSS jammers, which are often used for disrupting vehicle tracking systems.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

The spectrogram below provides an example of one such automotive jamming event, showcasing its notable and popular type of modulation.



© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

6. Comparison of Detected GNSS Interference with ADS-B Data

In this section, we compare the **major** GNSS interference events detected using our terrestrial monitoring system with ADS-B-based interference data from the spoofing.skai-data-services.com platform.

Throughout the observation period, we consistently detected two primary types of GNSS interference signals that exhibited stable characteristics and repeatability:

- **Multi-Constellation Jammer**: This interference type was predominantly observed in June and July, as well as in August and September.
- **Multi-Tone Interference**: First detected in October, this signal was identified multiple times in subsequent months.

Below is a summary of the major long-duration interference events detected by our system, including their start time, end time, duration, and modulation type.

Event	Start Time (CET)	End Time (CET)	Duration	Modulation Type
June 27–28	June 27, 22:25	June 28, 06:09	**7h 44m**	Multi-Constellation Jammer
July 6–7	July 6, 22:34	July 7, 03:04	**4h 30m**	Multi-Constellation Jammer
July 8–9	July 8, 22:25	July 9, 04:52	**6h 27m**	Multi-Constellation Jammer
July 15–16	July 15, 23:33	July 16, 06:22	**6h 49m**	Multi-Constellation Jammer
July 27	July 27, 03:11	July 27, 23:37	**20h 26m (intermittent)**	Multi-Constellation Jammer
August 15	August 15, 19:30	August 15, 21:50	**2h 20m**	Multi-Constellation Jammer

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

September 17–18	September 17, 23:10	September 18, 06:05	**6h 55m**	Multi-Constellation Jammer
October 15	October 15, 03:30	October 15, 06:05	**2h 35m**	Multi-Tone
October 22	October 22, 07:01	October 22, 10:48	**3h 47m**	Multi-Tone
October 23	October 23, 10:14	October 23, 14:30	**4h 16m**	Multi-Tone
October 27 (night)	October 27, 01:24	October 27, 08:51	**7h 27m**	Multi-Tone
October 27 (evening)	October 27, 17:30	October 27, 23:42	**6h 12m**	Multi-Tone
November 4	November 4, 12:45	November 4, 15:50	**3h 5m**	Multi-Tone

6.1 Methodology for Comparing Terrestrial and ADS-B Data

The spoofing.skai-data-services.com platform provides ADS-B-based GNSS interference detection, but its dataset has several limitations:

1. **ADS-B data does not provide real-time information** since the results are based on statistical post-processing.
2. **Only medium-high-altitude interference can be analyzed**, meaning low-power jamming sources affecting ground-level GNSS infrastructure may remain undetected.
3. **The platform does not classify interference modulation**, making it impossible to directly compare signal characteristics.

Due to these limitations, our comparison approach is based on pattern correlation:

- For each detected GNSS interference event, we will compare ADS-B data trends from the day before, during, and after the event.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

- Specifically, we will analyze the density of red squares on ADS-B interference maps, which indicate increased jamming intensity.
- If the ADS-B data shows a visible pattern change during a terrestrial interference event, this would indicate that the same interference likely impacted both high-altitude and ground-level systems.
- If no significant pattern change is observed, it would suggest that the interference was localized at ground level and did not propagate strongly to higher altitudes.

6.2 Comparison of Terrestrial and ADS-B Data

To assess whether high-altitude ADS-B data reflects the GNSS interference detected by our terrestrial monitoring system, we manually reviewed ADS-B interference maps for each observation period. This process involved browsing through daily ADS-B data, day by day, across the observation timeframe.

Despite this extensive review, no clear correlation was found between the interference events detected by our ground-based system and the ADS-B interference maps. In particular, even during periods of strong and prolonged jamming, as recorded by our system, there was no obvious increase in ADS-B jamming indicators on the corresponding days.

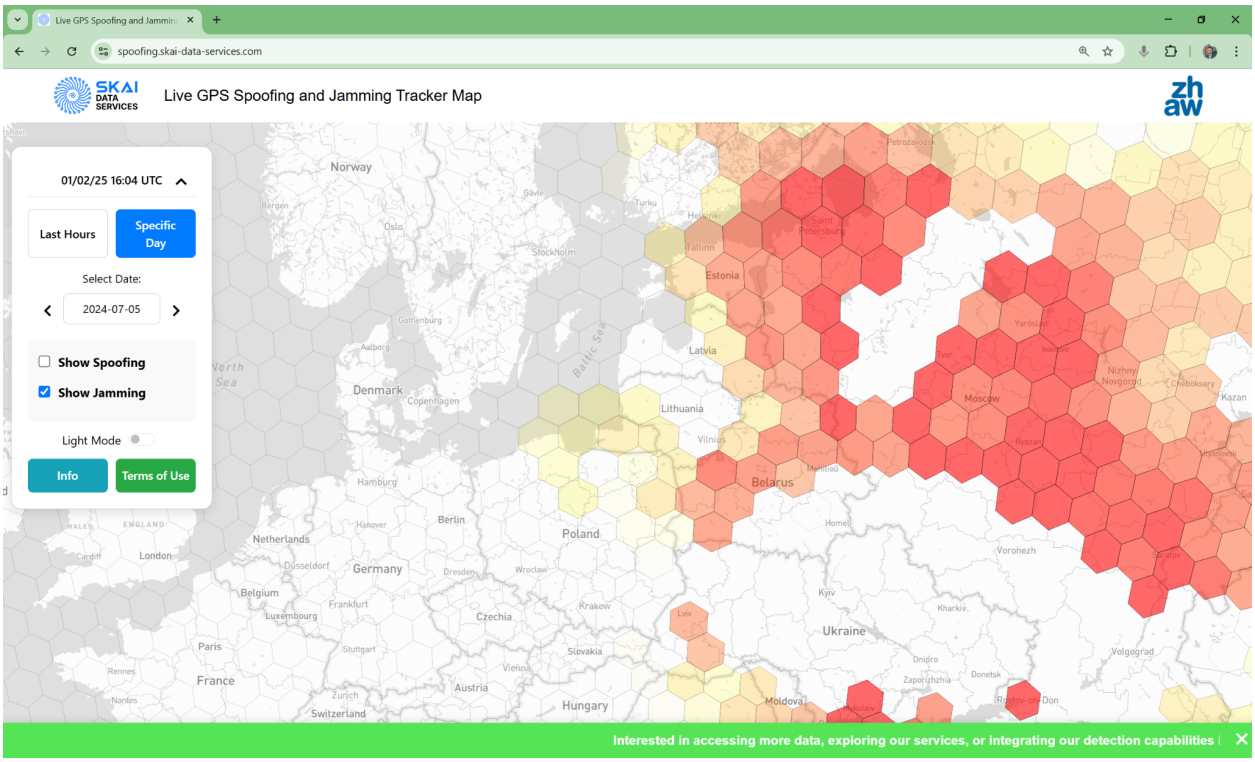
However, it is important to note that this type of comparison has inherent limitations:

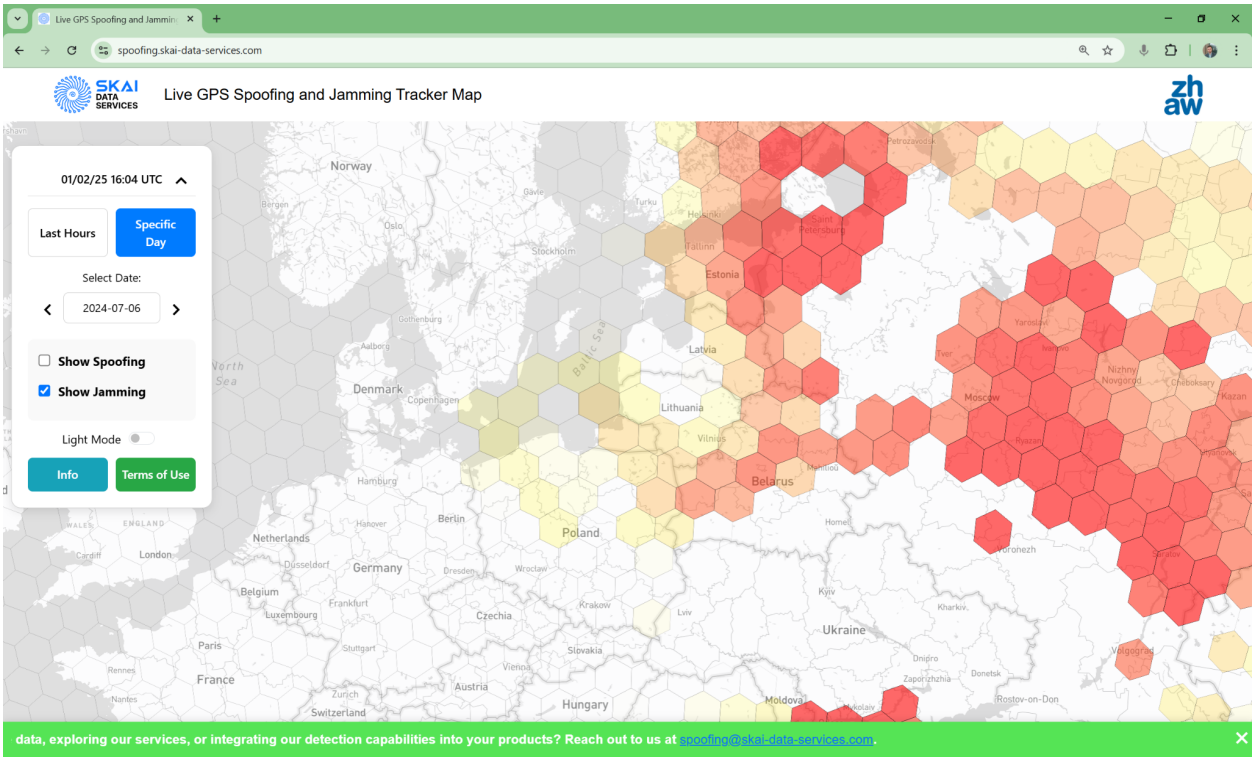
- The ADS-B dataset provides only a daily statistical summary, making it difficult to extract precise temporal correlations.
- The ADS-B visualization is static, lacking detailed breakdowns of interference intensity variations within a single day.
- The absence of raw numerical data or time-series analysis tools in the ADS-B platform further restricts in-depth comparisons.

For example, the ADS-B jamming data from July 5 to July 10 shows no clear visual indication of major interference, despite our system detecting a strong and extended jamming event from July 6 at 22:34 to July 9 at 04:52. This discrepancy suggests that the interference affecting ground-based GNSS users does not necessarily impact high-altitude ADS-B receivers, or that ADS-B data processing may smooth out short-term interference events.

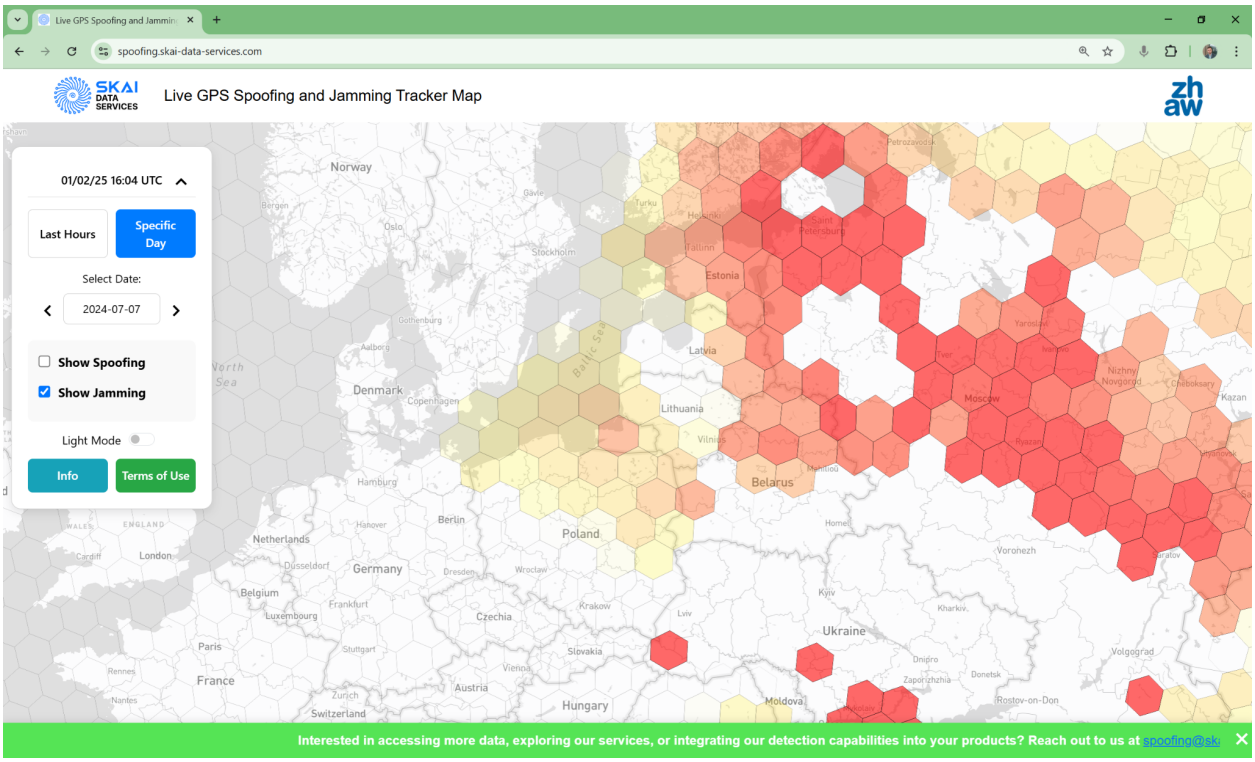
While this analysis does not rule out all possible correlations, it confirms that no obvious direct relationship exists between the interference detected at ground level and ADS-B-based interference indicators during the studied period.

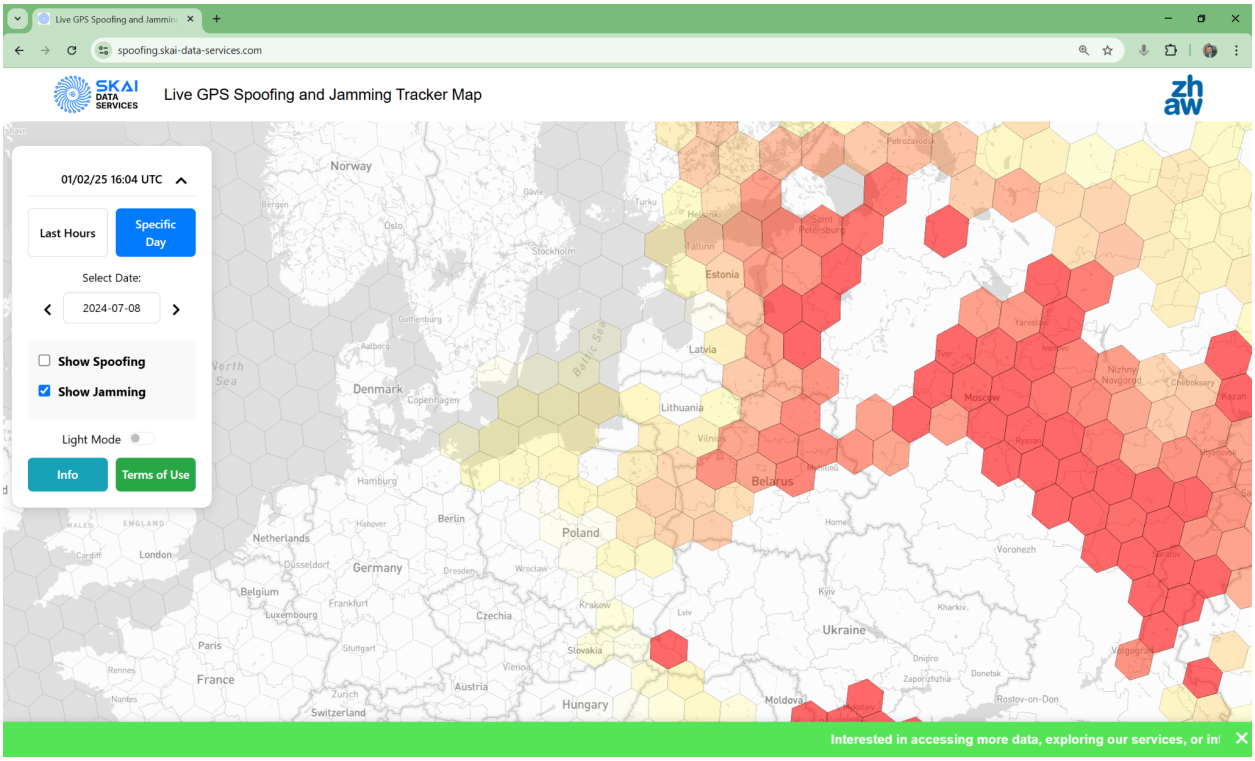
© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.



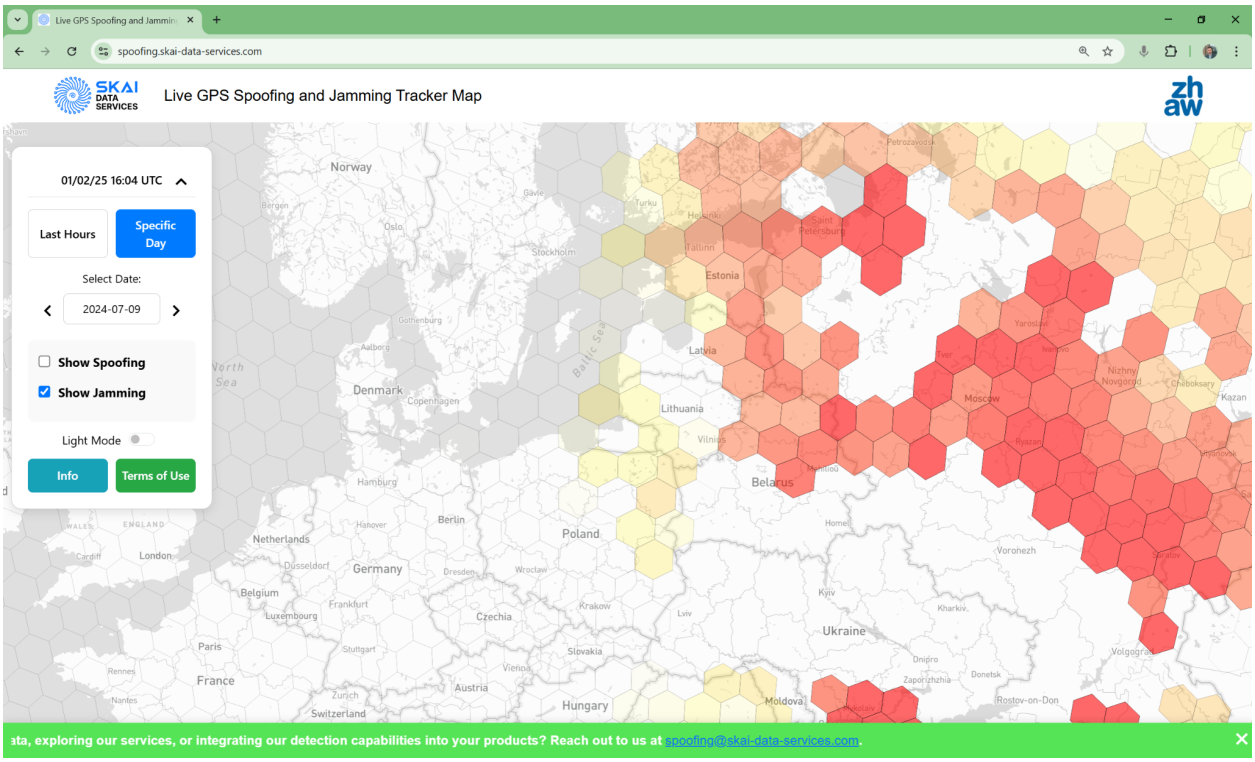


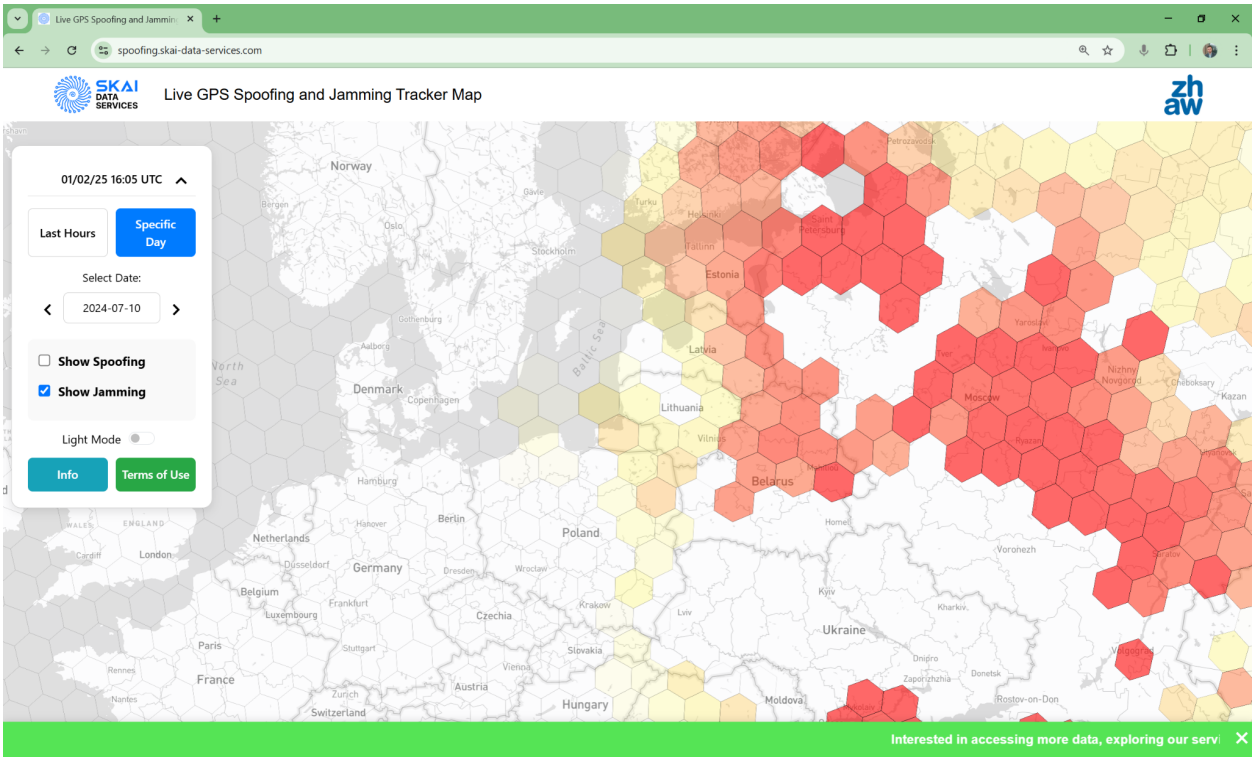
© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.





© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.





© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

7. Findings and Conclusion

Summary of Detected Interference

Over the observation period, a total of 84 hours of GNSS interference were detected, with jamming accounting for the majority of disruptions. Two dominant modulation types were observed:

- Multi-Constellation Jammer – primarily detected in June, July, August, and September, characterized by interference affecting multiple GNSS constellations simultaneously.
- Multi-Tone Interference – first detected in October, showing a shift in jamming techniques with stronger signal suppression characteristics.

The total number of long-duration interference events was 13, with an average duration of 5 hours and 50 minutes per event. These extended disruptions present a serious risk to GNSS-dependent infrastructure, particularly along the coastal regions, where maritime navigation, port operations, and timing-based systems rely heavily on GNSS accuracy.

Impact on GNSS Performance

Even when interference was not strong enough to fully block GNSS signals, certain modulation types significantly degraded positioning/timing accuracy. Some interference events resulted in coordinate accuracy dropping from 3–5 meters to over 35 meters, which can be critical for applications requiring precise timing and positioning, such as:

- Maritime navigation in confined waterways.
- Port automation and cargo handling systems.
- Timing synchronization for communication networks and financial transactions.

No Correlation Between Terrestrial and ADS-B Data

Analysis of ADS-B interference reports did not reveal any clear correlation with the interference detected by our terrestrial monitoring system. Despite strong jamming events recorded at ground level, the ADS-B jamming maps did not show any corresponding increase in interference activity.

This reinforces the conclusion that ADS-B-based interference monitoring is insufficient for detecting ground-level GNSS disruptions. The lack of real-time data and the reliance on statistical post-processing further limits the usefulness of ADS-B reports for assessing real-world interference risks.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

Likely Source of Interference

Based on signal characteristics, it is highly likely that the primary source of interference is a GNSS jammer installed on one or more vessels operating in the Baltic Sea. The following observations support this hypothesis:

- The same Multi-Constellation Jammer pattern was detected multiple times across different months.
- Consistent movement patterns were observed, indicating that the source was likely mobile.
- The switch to Multi-Tone Interference in October suggests a change in equipment or jamming tactics, possibly indicating the use of more advanced jamming technology.

Whether this interference comes from a single vessel or multiple ships using similar jamming equipment remains unclear. However, the consistent nature of the signals suggests a coordinated or repeated source rather than random industrial noise.

The Necessity of a Full-Scale Terrestrial GNSS Interference Monitoring System

Our findings underscore the urgent need to establish a comprehensive territorial GNSS interference monitoring network along the Baltic Sea coast. The presence of persistent and mobile jamming sources poses a significant risk to maritime navigation, port operations, and other critical GNSS-dependent infrastructure. Given the limitations of airborne ADS-B-based monitoring in detecting ground-level interference, a dedicated high-density sensor network is essential to provide reliable, real-time situational awareness and ensure effective countermeasures.

A robust monitoring system should incorporate a high-density deployment of GNSS interference detection sensors strategically positioned along the coastline. The primary objectives of such a system would include:

1. **Precise Geolocation of Interference Sources Using TDOA Methods** – By leveraging time difference of arrival (TDOA) techniques, a network of widely distributed sensors can accurately pinpoint the geographic origin of interference sources. This capability is critical for identifying and mitigating unauthorized jamming activities that threaten maritime and terrestrial GNSS applications.
2. **Real-Time Tracking of Mobile Interference Sources** – Our study suggests that GNSS jammers are likely installed on vessels operating in the Baltic Sea. A high-density monitoring network would enable continuous tracking of these sources, allowing authorities to correlate interference patterns with vessel movement and take necessary actions to mitigate threats.
3. **Enhanced Protection of Critical Infrastructure** – Ports, offshore platforms, and coastal communication hubs depend heavily on uninterrupted GNSS functionality. A dedicated monitoring system would provide an early warning mechanism, allowing operators to respond promptly to interference events and minimize potential disruptions.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.

4. **Data-Driven Policy and Regulatory Enforcement** – A continuous monitoring network would generate valuable datasets to support regulatory agencies and policymakers in enforcing GNSS protection measures. By documenting interference incidents with high spatial and temporal accuracy, authorities can take evidence-based actions against illicit jamming activities.
5. **Integration with Maritime Traffic and Security Systems** – A territorial GNSS interference monitoring system could be integrated with existing maritime traffic control and security networks. This would facilitate coordinated responses between port authorities, coast guards, and regulatory bodies, enhancing overall situational awareness and maritime safety.

Given the increasing reliance on GNSS for positioning, navigation, and timing applications, the deployment of a full-scale, ground-based interference monitoring system is not just a technical necessity but also a strategic imperative. Establishing such a network along the Baltic Sea coast would significantly enhance the resilience of regional GNSS infrastructure, ensuring uninterrupted service for maritime operations, logistics, and other essential industries that depend on precise positioning and timing data.

© 2025 GPSPATRON and Gdynia Maritime University. All rights reserved. This report, including all data and illustrations, is the joint property of GPSPATRON and Gdynia Maritime University.