# GNSS INTERFERENCE AT-SEA NEAR KALININGRAD

## REVEALED BY SHIPBORNE TECHNOLOGY OF GPSPATRON DURING JUNE THROUGH OCTOBER 2025

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 USA and North America distributor of GPSPATRON Sp. z o. o.

# GNSS Interference Monitoring in the Baltic Sea: Shipborne Observations near the Kaliningrad Enclave Marine Border

## Observation period: 23.JUN.2025 – 14.OCT.2025

Date: 27.11.2025 Doc. revision: 1.3


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/

# Executive Summary

This joint report by GPSPATRON and the Gdynia Maritime University presents the most detailed and revealing picture to date of GNSS interference in the southern Baltic Sea, particularly in the maritime areas of The Gulf of Gdansk close to the marine border of the Kaliningrad Russian enclave. Building on our previous six-month land-based study—where only classical wideband jamming was observed—this new shipborne investigation uncovers a dramatic shift in the interference environment.

**A Transition From Simple Jamming to Advanced Spoofing**

Unlike the earlier coastal campaign, where every recorded event was pure jamming, the new data shows that all major interference episodes combined **GPS spoofing with multi-constellation jamming**. The GPS signal is forged, while GLONASS, Galileo, and BeiDou are simultaneously suppressed.

**The Most Intense GNSS Disruptions on Record**

The opening phase of the campaign—from late June through July—was the most severe, with GNSS availability **dropping to 83.2%,** meaning that only 83.2% of the time the system observed no interference. During this interval alone, the vessel recorded 4 days, 5 hours, and 24 minutes of GPS spoofing.

The single most extreme episode occurred between 1 and 3 June, where nearly 30 hours of spoofing were detected within a 48-hour window. For any maritime operator, such a prolonged GNSS disruption represents a serious navigational risk.

**A Coordinated Network of Four Distinct Interference Sources**

Spectrogram analysis reveals that the interference originates not from one emitter but from four separate and technologically distinct systems operating in synchrony:

1. GPS spoofing transmitter – generating forged GPS L1 signals.
2. Lower-band chirp jammer – targeting GPS, Galileo, and BeiDou.
3. Upper-band chirp jammer – targeting GLONASS exclusively.
4. Full-band analog-like jammer – flooding the entire 60 MHz GNSS L1 band.

These systems activate and cease simultaneously, yet differ in bandwidth, modulation, and spectral signature—clear evidence of a distributed, multi-station interference network with centralized tactical coordination.

## Evolution of GNSS Jamming Modulation

In our previous coastal study, the dominant jamming source was a high-quality, purpose-engineered wideband signal with three clean, constellation-matched components — a hallmark of modern, deliberately designed equipment. In the current campaign, however, this pattern has shifted toward simpler wideband chirp jamming, a less advanced technique but one deployed at much higher power levels.

The new interference environment is further strengthened by the addition of persistent GPS spoofing, a capability absent in the earlier study. Together, this marks a transition from refined, high-precision targeted jamming to a more complex, multi-emitter interference system, where chirp jammers and spoofers operate simultaneously to create a significantly more disruptive operational impact.

## Interference Intensifies as Vessels Leave the Coast

A strong geographic pattern was recorded:

- In the Port of Gdańsk, the interference is weak or barely visible.
- In open water, the same signal becomes up to 15 dB stronger.
- Interference strength consistently increases when approaching the waters facing Kaliningrad.

This means that, intentionally or not, the interference system targets maritime traffic far more than coastal infrastructure.

## Unintentional Interference in Port: Automotive and Industrial Signals

Even without strategic systems, the port environment contains its own risks:

- Automotive jammers carried by civilian vehicles (cars, taxis, trucks) generated repeated short bursts of GNSS disruption.
- Industrial RF noise, appearing in multi-hour intervals on 3, 5, and 10 September, produced broadband emissions consistent with malfunctioning electrical or RF equipment.

These non-military sources highlight that GNSS interference is not exclusively a geopolitical issue—even ordinary port activity introduces additional noise into the spectrum.

**Implications for Maritime Safety in the Southern Baltic**

The findings of this study show that the GNSS environment in the southern Baltic is undergoing a clear transformation. The emergence of combined spoofing–jamming interference, the operation of multiple spatially separated emitters, and the increase in interference power indicate that vessels in this region may encounter degraded or unreliable GNSS information more frequently than before.

The shipborne measurements collected in this campaign confirm that:

- GNSS integrity cannot be taken for granted, particularly in waters facing the Kaliningrad region.
- Shore-based monitoring provides only a partial picture; offshore conditions can differ significantly and require direct measurement from vessels.
- Onboard interference awareness tools can meaningfully support navigators, helping them correctly interpret navigation data and maintain situational awareness.

An important operational aspect is that spoofed GNSS positions may propagate directly into the AIS ecosystem, affecting systems that rely on GNSS/AIS alignment. While trained navigators can operate safely without GNSS, awareness of potential inconsistencies remains essential for effective bridge management.

When falsified GNSS positions appear in AIS, several practical challenges may arise:

- Misaligned positional awareness, requiring cross-checks with radar, visual bearings, and other independent sources.
- Phantom or misreported targets, complicating traffic-management decisions.
- Reduced clarity in low visibility, when diverging navigation inputs require closer attention.
- Potential impact on automated systems, where CPA/TCPA or autopilot outputs may need verification.

The Gulf of Gdańsk is a busy corridor with significant commercial and industrial traffic. For vessels carrying hazardous or high-value cargo, redundancy in navigation inputs remains important for safe operation.

Overall, this study does not suggest that navigation in the southern Baltic has become unsafe, but it does show that the region is experiencing more frequent and more complex GNSS disturbances. Mariners, VTS authorities, and port operators can benefit from access to real-time interference information, reliable alerting tools, and procedures for cross-checking navigation sources whenever GNSS integrity is in doubt.

The overarching conclusion is clear: GNSS interference is now an operational factor in the southern Baltic, and informed awareness—rather than alarm—is the most effective response.

# 1. Introduction

This report is a continuation of the joint research initiative conducted by GPSPATRON and Gdynia Maritime University on GNSS interference in the Baltic Sea region. In our previous study, *"Report on GNSS Interference in the Baltic Sea: Analysis Using a Terrestrial Monitoring System and Comparison with ADS-B Data"* , we presented a six-month ground-based analysis of GNSS disruptions recorded at the Faculty of Navigation in Gdynia. That study revealed several key findings, including:

- Persistent **multi-constellation jamming** affecting GPS, Galileo, Beidou and GLONASS with chirp and multi-tone modulation.
- Evidence pointing to **mobile maritime sources** as the most probable origin of several long-duration interference events.
- A **lack of correlation** between terrestrial GNSS disturbances and ADS-B-based interference maps, confirming that high-altitude monitoring cannot reliably detect threats affecting ground-level and maritime operations.

Building on this foundation, the present report represents the **second phase** of our collaborative research. In this phase, the GP-Probe TGE2 interference sensor was installed **on board a research vessel** operating in the southern Baltic Sea, with regular transits **toward the maritime border of the Kaliningrad region**. The purpose of this deployment was to collect higher-quality GNSS interference data and reduce the distance to potential interference sources.

By transitioning from a stationary coastal sensor to a **mobile, shipborne measurement platform**, this phase of the study allows us to record GNSS interference in the **exact operational environment** where maritime crews are most likely to encounter it. A sensor installed on a vessel experiences the same propagation conditions, signal masking, multipath effects, and line-of-sight dynamics that affect GNSS receivers onboard real ships. This makes the collected interference data significantly more representative for practical navigation scenarios. It also enables us to capture jamming and spoofing signals that **would not be observable** from a fixed land-based location due to the different radio horizon and spatial position of the vessel. As a result, the shipborne dataset provides higher value for maritime operators, as it characterizes interference exactly as it impacts onboard equipment.

The measurements presented in this report were collected between **23 June and 14 October 2025**, during regular research voyages along the Polish coastline and multiple approaches toward the maritime boundary with the Kaliningrad region.

# 2. Shipborne Installation

The GNSS interference detector was installed directly on the research vessel, where it operated throughout the entire observation period. The photos show the vessel itself, the mounting locations of the GNSS antennas, and the installation of the GP-Probe TGE2 sensor.

The photograph shows **three GNSS antennas installed on the main mast of the vessel**, mounted on horizontal support bars at different heights. Their elevated placement ensures unobstructed sky visibility and realistic reception conditions for shipborne GNSS equipment.

Used GNSS interference detector: **GP-Probe TGE2** installed within the vessel's equipment compartment:


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.**

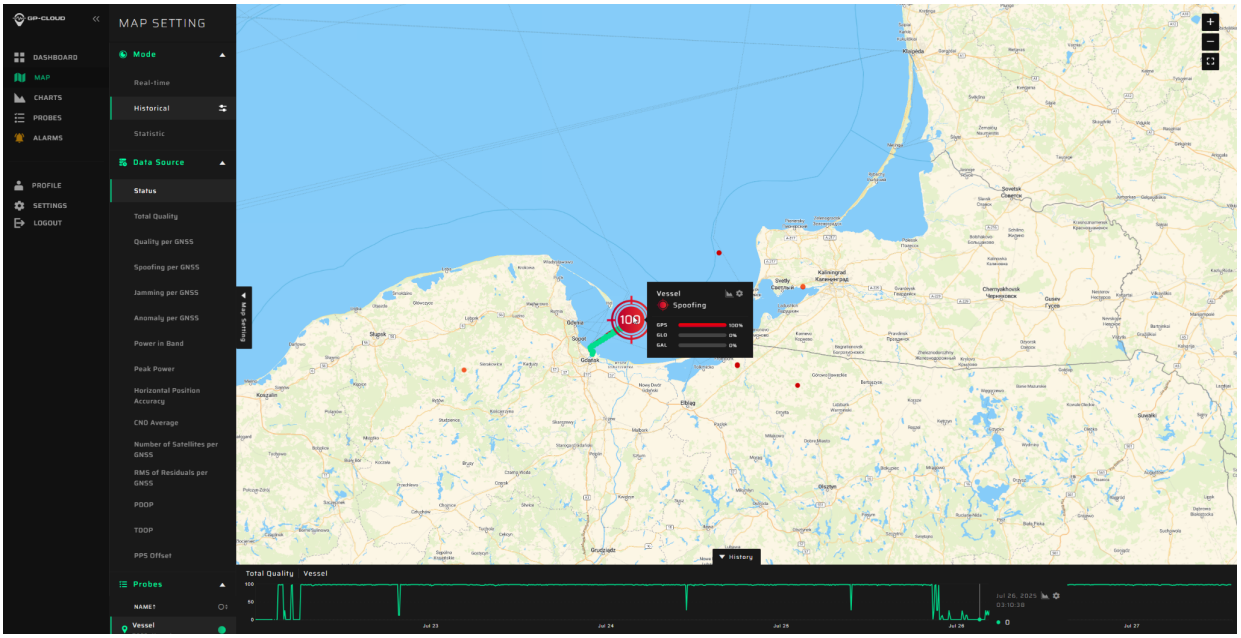
Technical Specifications:

- 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.

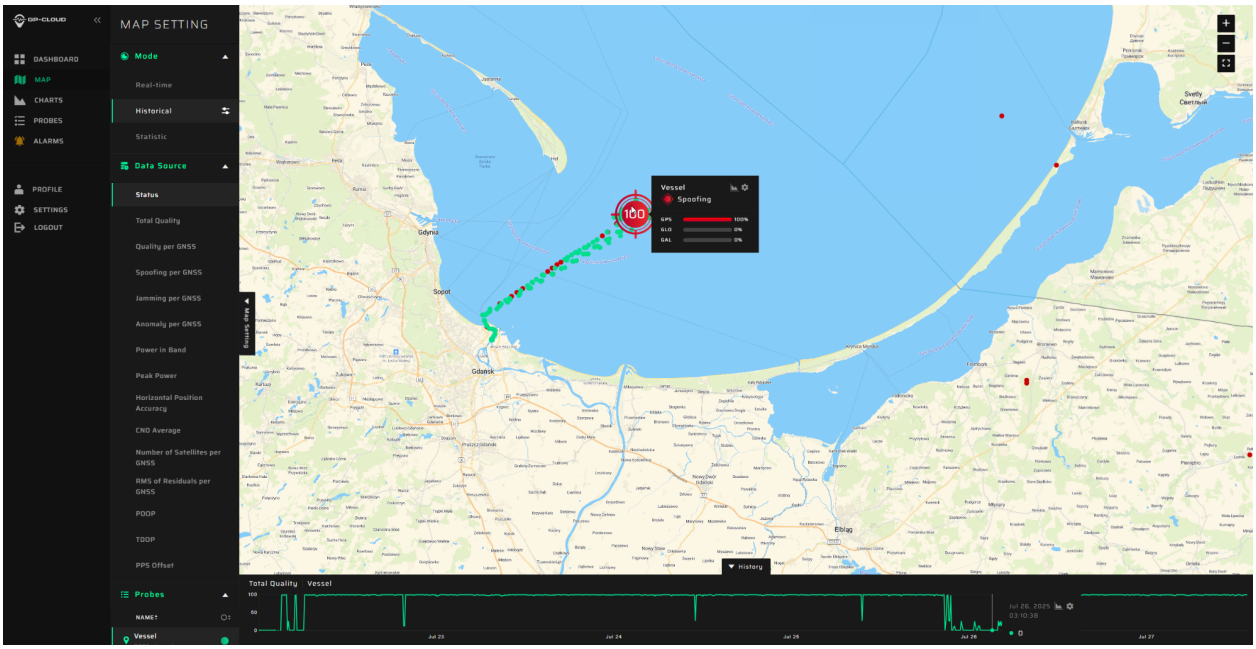
# 3. Patrol Areas Overview

During the campaign, the vessel was berthed in the Port of Gdańsk between offshore operations, and the GNSS interference detector operated continuously throughout the entire period. After leaving the port, the vessel proceeded directly to its designated offshore observation area in the outer part of the Gdańsk Bay, where it performed maneuvering within a relatively confined zone during each measurement session.

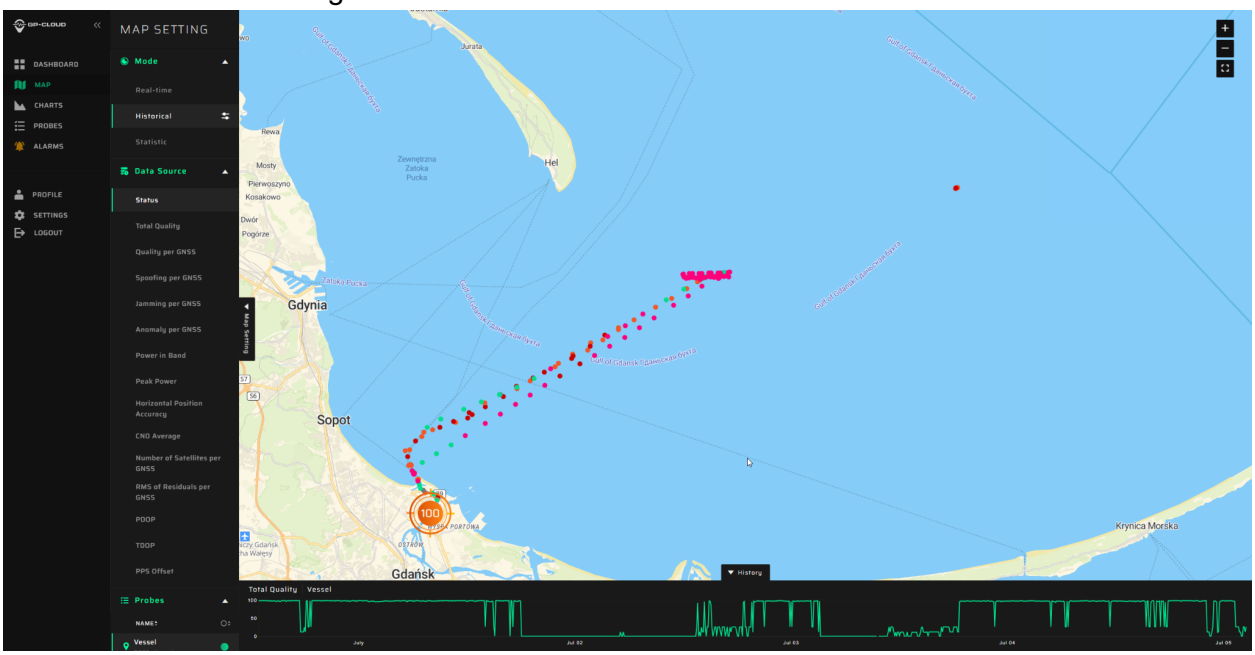
Most offshore activity took place in **July**, when the vessel frequently operated in the observation area for extended periods. From **August to October**, it remained in port more often, leaving for offshore measurements only occasionally. As a result, the dataset collected for this report combines both coastal and offshore conditions, offering a cumulative view of GNSS interference recorded near the shoreline and at sea.




The vessel's offshore position was located approximately **42–47 km** from the Poland–Russia maritime border and **55–60 km** from the nearest coastline of the Kaliningrad Region. This vantage point provides a realistic representation of GNSS conditions experienced by vessels navigating in the approaches to the Port of Gdańsk and Port of Gdynia. Because the measurements were taken directly at sea, away from land-based obstructions, they reflect the true operational GNSS environment encountered during offshore maneuvering and approach phases. For captains and navigation officers, this offers significant practical value: the data characterizes GNSS performance exactly where ships commonly operate while waiting for clearance, preparing to enter port, or conducting tasks in the outer bay area.




The vessel's maneuvering zone:




The ship often remained in this zone for several hours before returning to the Port of Gdańsk. Depending on operational plans, multiple trips per day were possible, although there were no consistent patterns.

# 4. Monthly GNSS Interference Overview

This section provides a month-by-month statistical analysis of all GNSS interference events recorded during the observation period. The metrics shown here include data captured both while the vessel was berthed in the Port of Gdańsk and during offshore operations in the Gdańsk Bay, offering a combined view of coastal and at-sea conditions.

It is important to note that the vessel spent the majority of its active measurement time in **late June and July**, when it frequently operated in the offshore observation area. In August through early October, the vessel remained in port for longer periods, conducting offshore measurements less often. As a result, the monthly statistics reflect the actual operational pattern of the campaign, with more extensive sea-based data in June–July and a higher proportion of port-side data in the following months.

For each month, a spectrum waterfall and a spoofing detection probability timeline are presented, providing a visual overview of interference characteristics and their temporal distribution.

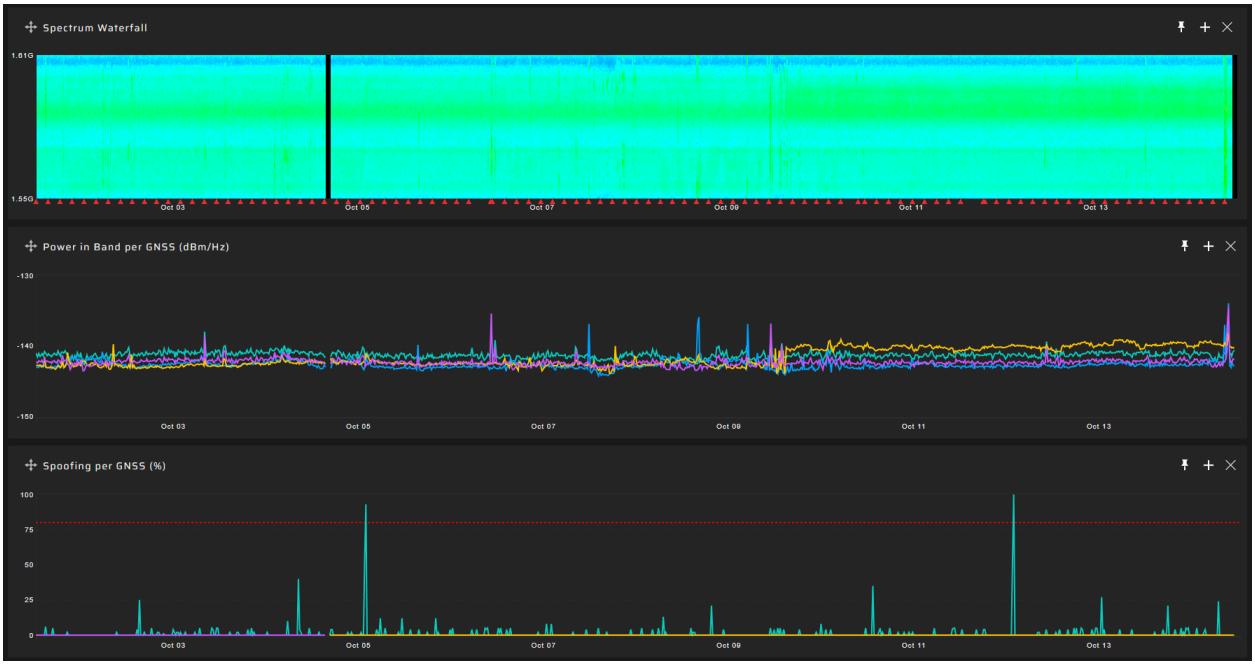
**Late June & July Combined Overview (Most Measurements Collected Offshore):**


June–July recorded the highest number of interference events and the strongest signal levels, largely because the vessel spent the most time at the offshore observation position. Even without considering the longer measurement time at sea, it is clear that June and July were the most active and challenging months in terms of GNSS interference.

## August (Two Offshore Trips Early in the Month):


## September (Single Offshore Trip in the Second Half of the Month):

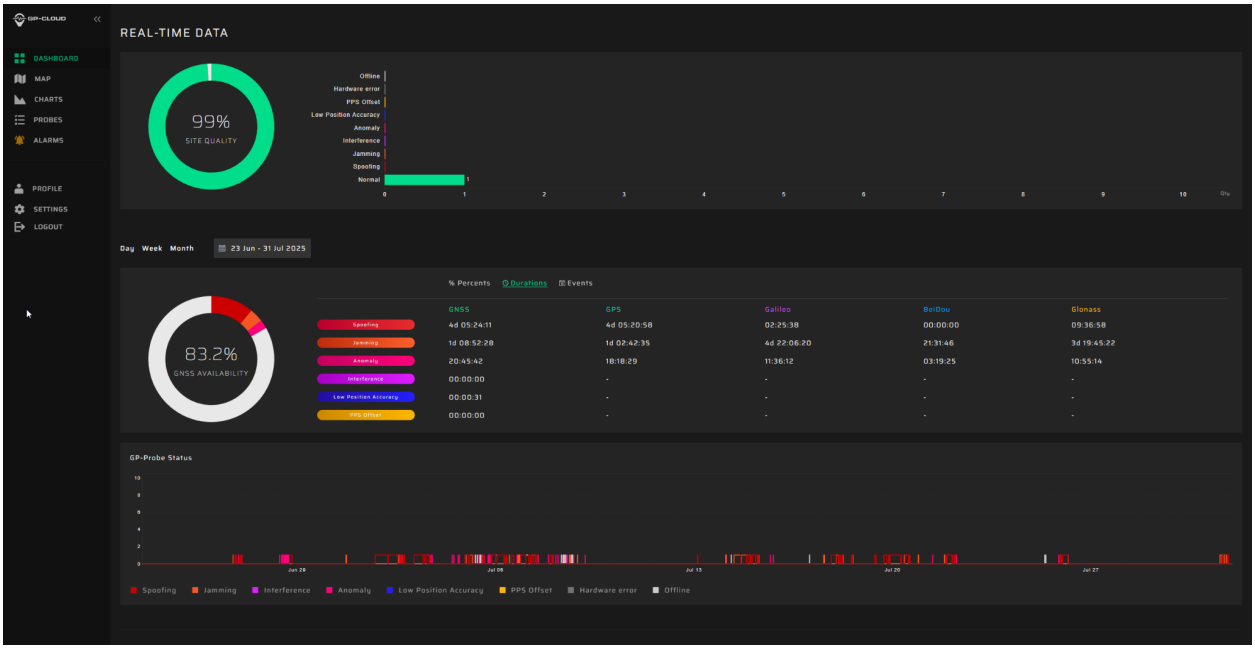
**October. 1–14 October Only (Vessel Remained in Port Throughout the Period):**




The following table summarizes the monthly spoofing durations, jamming durations, and GNSS availability for the entire observation period.

| Period | Spoofing Duration | Jamming-Only Duration | GNSS Availability, % |
|---|---|---|---|
| Late June & July (majority offshore) | 4d 05:24:11 | 1d 08:52:28 | 83.2% |
| August (two offshore trips early in the month) | 1d 00:08:33 | 1d 07:06:56 | 91.72% |
| September (single offshore trip in second half) | 11:44:47 | 10:39:31 | 96.58% |
| October (1–14) (vessel remained in port) | 00:01:41 | 09:25:45 | 96.97% |

The end of June and the entire month of July were the most active periods of the observation campaign, both in terms of the number of interference events and their power levels. This is partly due to the fact that the vessel spent the most time in the offshore observation area, where interference is captured more clearly and with higher signal strength. However, even without this operational factor, the overall interference environment in late June and July was objectively the most intense.




In August, interference activity remained elevated, especially in the first half of the month, when several long-duration and clearly structured events were recorded. Yet, because the vessel stayed mostly in port, these events appear less pronounced on spectrum visualizations due to reduced received power levels in the harbor environment.

In September, only one major offshore interference event was detected, corresponding to the vessel's single offshore trip during the second half of the month. Nevertheless, the overall interference background during September remained complex: numerous weaker disturbances were visible even while the vessel was berthed in the port, although their power levels were significantly attenuated compared to offshore conditions.

October was generally quiet, with the vessel remaining in port throughout the first half of the month. No strong interference events were detected. However, starting from around October 10th, intermittent low-power disturbances appeared in the GLONASS band, exhibiting a Gaussian-like modulation structure. These signals were weak and only faintly visible in the data due to the vessel's position inside the port.

# 5. Interference Intensity vs. Vessel Location

To demonstrate how GNSS interference evolves as a vessel moves away from the coast and approaches the open Baltic Sea, we selected a specific interference episode in which **the same signal, with the same structure and spectral signature**, was recorded twice: first while the vessel was berthed in the Port of Gdańsk, and later—after leaving the port—at the offshore observation area. This allows for a direct, controlled comparison of signal strength and signal clarity under identical interference patterns.

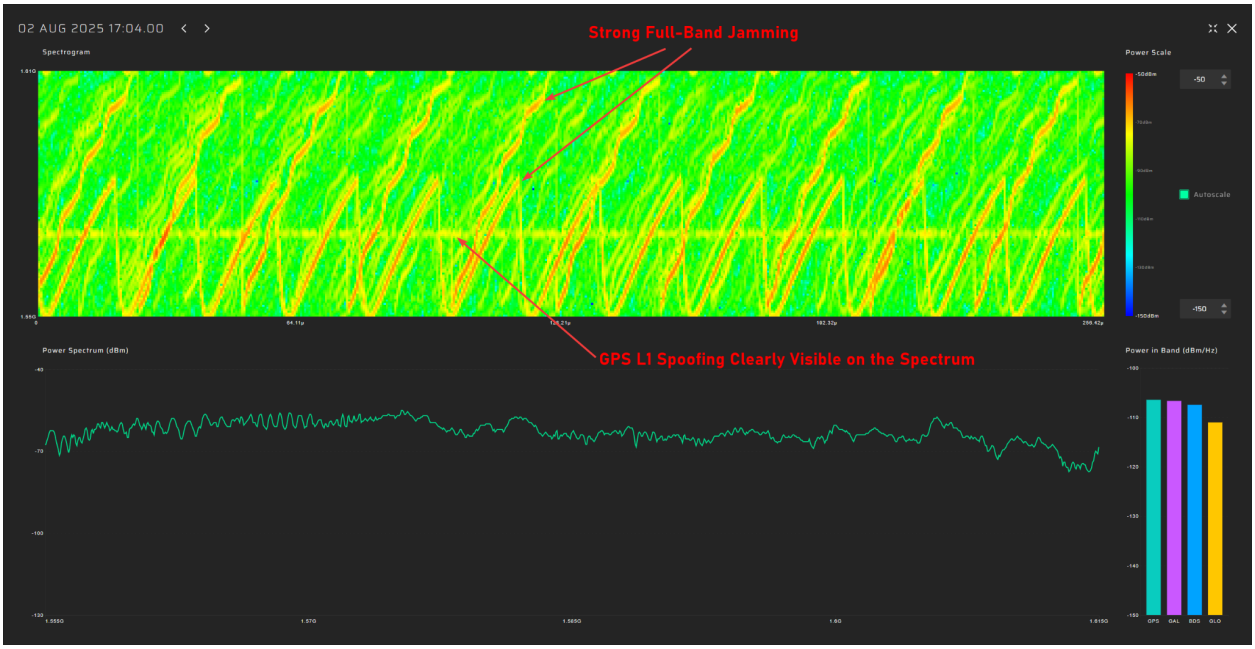
On the left, the interference recorded in port is displayed; its spectral signatures are recognizable but faint. On the right, the exact same interference pattern, recorded offshore, appears twice with identical waveform structure and spectral features—but at a much higher power level.


Analysis of these two recordings shows that the offshore version of the same interference signal is, on average, approximately **15 dB stronger** than the version recorded in port. This confirms a clear trend: as the vessel exits the Gdańsk Bay and moves toward open sea, the received interference power increases, indicating that the source of this signal—likely located in or near the Kaliningrad region—becomes progressively more powerful.

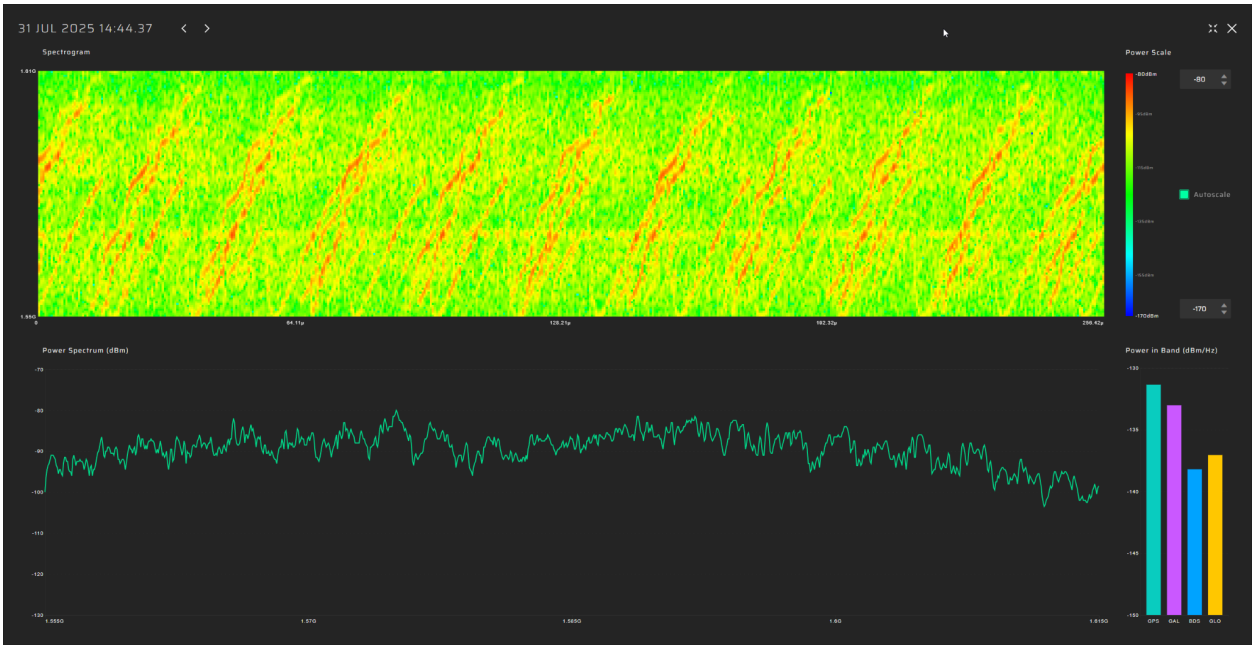
While the interference is still detectable in port, the spoofing component is extremely weak, and our detector registers only occasional minor spoofing triggers. In contrast, once offshore, both spoofing and jamming components become clearly visible and easily classified, demonstrating that these signals are strong enough to meaningfully affect maritime GNSS receivers operating at sea.

**The offshore spectrogram** clearly reveals three distinct components:

- A wideband, full-band jamming signal affecting all GNSS constellations simultaneously.
- A narrower jamming signal affecting GPS and BeiDou but not GLONASS, indicating selective or band-limited interference.
- A GPS L1 spoofing signal, distinctly visible even on the spectrum itself.




**Port recording** — same interference pattern, but significantly weaker signal



# 6. GNSS Interference Classification and Detailed Signal Analysis

In this section, we present a detailed analysis of one representative interference incident. Although multiple events were recorded during the campaign, all of them share the same characteristic structure. Therefore, analyzing a single episode is sufficient to demonstrate the full behavior of GNSS interference patterns occurring in the region. The chosen incident is illustrative of the typical spoofing and jamming configuration repeatedly observed both in port and offshore.

## 6.1 Signal Classification: Spoofing and Multi-Constellation Jamming

Our system identified a persistent GPS spoofing signature occurring simultaneously with multi-constellation jamming targeting all other GNSS systems. The GP-Cloud screenshot clearly shows strong and consistent signatures of GPS spoofing together with multi-constellation jamming. This configuration is commonly observed in this region:


You can see that only GPS satellites remain visible, and they exhibit extremely large pseudorange residuals — a strong indicator of non-coherent spoofing. Despite the spoofed GPS signals being strong, their $C/N_0$ levels do not appear unnaturally high; instead, they are shaped to mimic realistic satellite signal strengths..

This spoofing–jamming combination is a widely used technique. Full multi-constellation spoofing would require generating all GPS, Galileo, GLONASS, and BeiDou signals across multiple

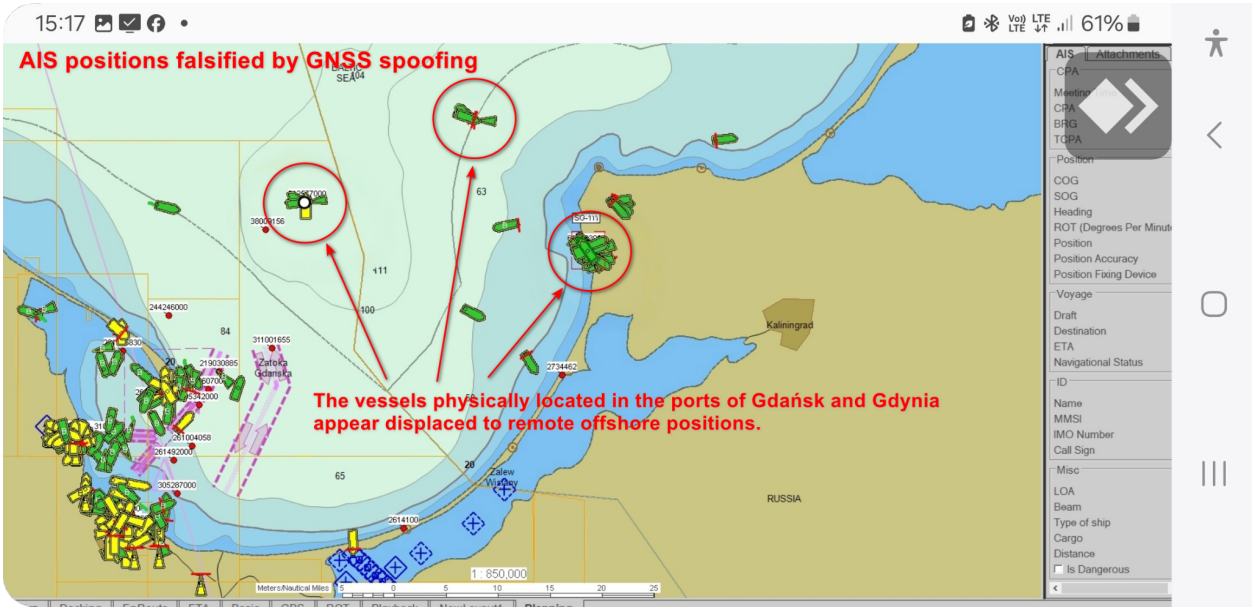
frequency bands (L1, L2, L5, E1, E5, G1, B1, etc.). Each signal type needs its own generator, power amplifier, and precise synchronization chain. In practice, this is complex and costly. For this reason, real-world interference systems typically spoof only GPS—the primary navigation constellation—and simultaneously jam all other GNSS signals. This prevents the receiver from performing any constellation cross-checks and forces it to rely solely on the forged GPS solution.

## 6.2 Vessel Position Errors Under GNSS Spoofing: Teleportation, Drift, and Circular Tracks

One of the most visible and operationally significant consequences of the spoofing events documented in this study is the false positional information reported by shipboard GNSS receivers and subsequently broadcast through the Automatic Identification System (AIS).

Because AIS simply transmits whatever position the onboard GNSS sensor provides, any falsified coordinates are automatically propagated to nearby vessels, VTS systems, and maritime traffic platforms.

**False AIS Positions (“Teleportation” Effect)**




The screenshot clearly demonstrates this behavior. Vessels that were physically located inside the ports of Gdańsk or Gdynia, or at their designated anchorages, suddenly appeared on AIS charts tens or even hundreds of kilometers away.

During spoofing intervals:

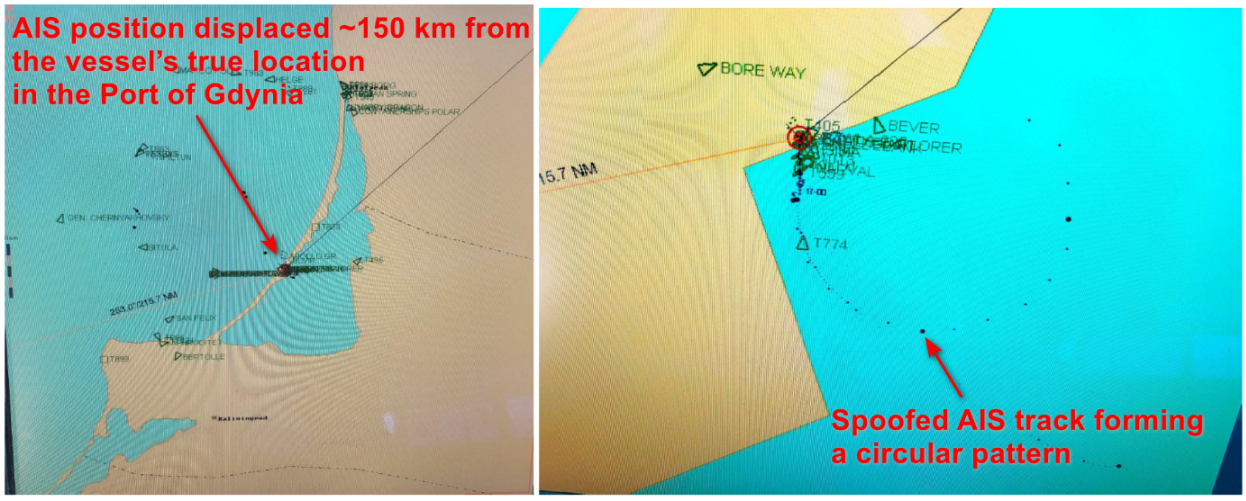
- All vessels within the spoofing footprint reported identical falsified coordinates, often in remote areas of the Baltic Sea or even on land.

- All GNSS receivers in the affected area were forced to accept the same forged GPS L1 solution.
- These falsified positions were then distributed through AIS as if they were real, creating the appearance that ships had “teleported” far from their actual locations.

### Circular Tracks and Drifting False Trajectories

One of the most used spoofing tactics—especially in systems designed to protect critical infrastructure from drones or missiles—is the creation of a **circular false trajectory**. This technique simulates a target moving at a constant altitude and velocity along a smooth circular path, producing GNSS data that appears physically plausible to onboard navigation filters. It is specifically designed to evade modern spoof-detection algorithms.

The screenshot included in this section illustrates exactly this behaviour:




- A vessel actually located in the Port of Gdynia was suddenly displaced more than 150 km toward the Kaliningrad region.
- After this initial “teleportation,” the falsified GNSS/AIS position began drifting in a circular pattern, generating a loop-shaped track entirely disconnected from the vessel’s real movement.

**Conclusion: Operational and Safety Risks for the Baltic Sea**

The evidence presented here demonstrates with absolute clarity that maritime GNSS receivers are highly vulnerable to spoofing, and that falsified coordinates enter the AIS network automatically, becoming indistinguishable from legitimate position reports.

In the high-density shipping corridor of the Gulf of Gdańsk, this poses a direct and growing threat to navigational safety.

Spoofed AIS data undermines the foundation of modern maritime operations. Most vessels today depend on automated systems that assume AIS/GNSS positions are reliable:

- Autopilots and integrated bridge systems
- Collision-avoidance tools (CPA/TCPA)
- ECDIS overlays and route optimization
- VTS surveillance and traffic management systems

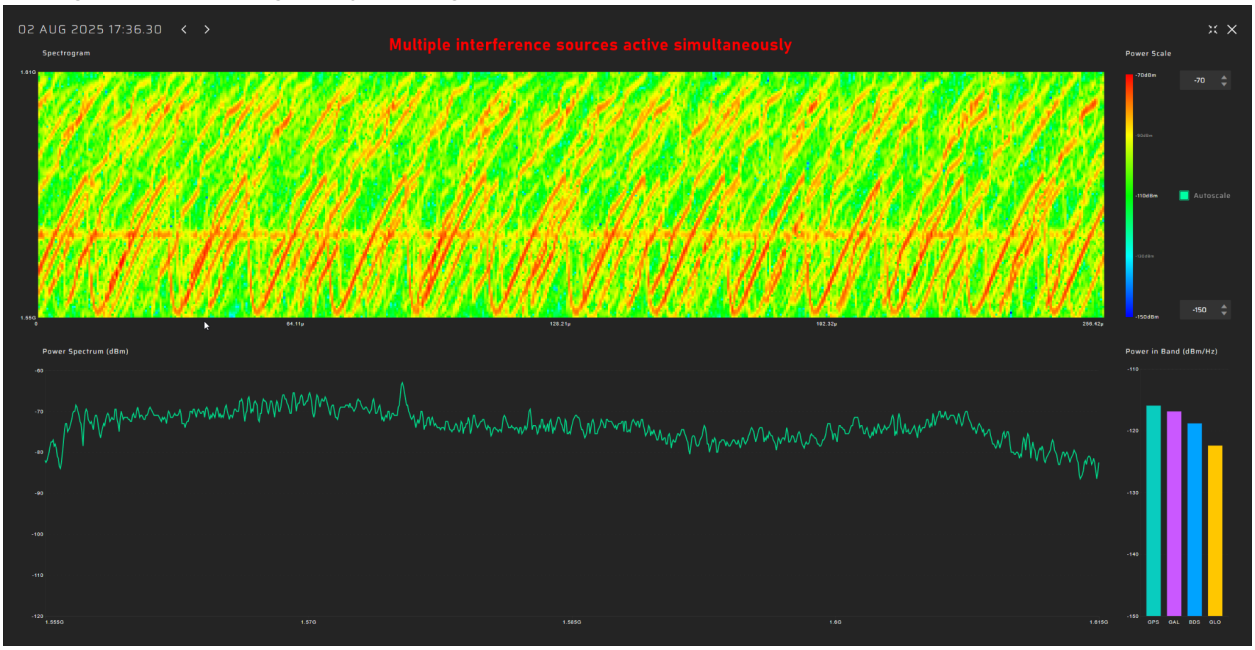
When false GNSS positions enter this ecosystem, the consequences can be severe:

- Hidden real positions: Ships may be physically in port while AIS shows them hundreds of kilometers away, eliminating situational awareness for both nearby vessels and traffic controllers.
- Phantom vessels in traffic lanes: Spoofed AIS tracks can generate “ghost ships,” obstructing routes and confusing VTS operators.
- Collision risk in low visibility: Fog, night operations, and winter conditions amplify the danger when navigation systems suddenly lose or corrupt the only electronic reference to the ship’s true position.
- Failure of automated safety systems: When GNSS/AIS inputs are falsified, autopilot systems and alarm logic can behave unpredictably—or fail completely.
- Hazards involving dangerous cargo: The Gulf hosts tankers, LNG carriers, chemical vessels, and military ships. A spoofing-related navigational accident involving such vessels could lead to major environmental damage, fires, explosions, or casualties.
- Escalating regional risk: As spoofing episodes expand in area, duration, and frequency, statistical trends across multiple industries show that serious accidents become inevitable.

In summary, the findings demonstrate that GNSS spoofing in the southern Baltic is not a theoretical threat—it is an operational reality already affecting vessels daily. The risks to maritime safety, port operations, and environmental security are immediate and significant.

## 6.3 Spectrogram Analysis

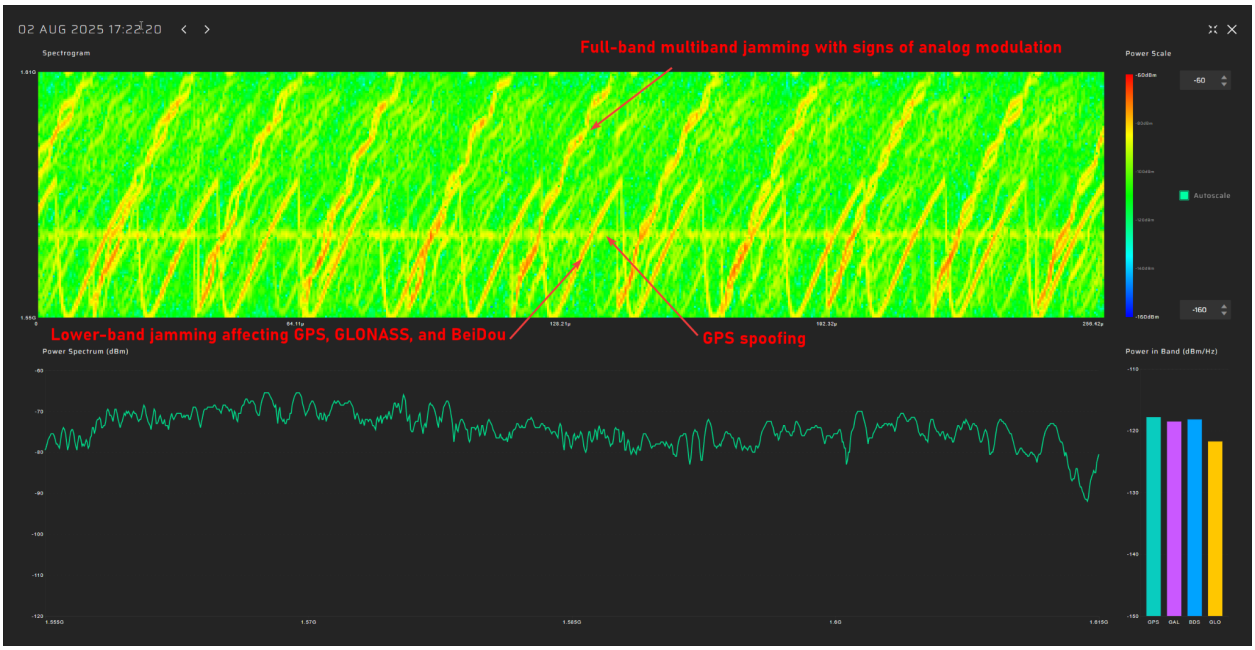
The spectrograms recorded during the campaign show that the interference environment in the region is complex and highly layered. Even a preliminary visual inspection reveals **multiple overlapping interference components with different spectral characteristics**, indicating that several electronic warfare systems may be operating simultaneously, affecting GNSS reception through both spoofing and jamming mechanisms:




On the first spectrogram, the situation is difficult to interpret due to the number of overlapping signals, so we selected additional spectrograms where the individual components are more clearly separated.

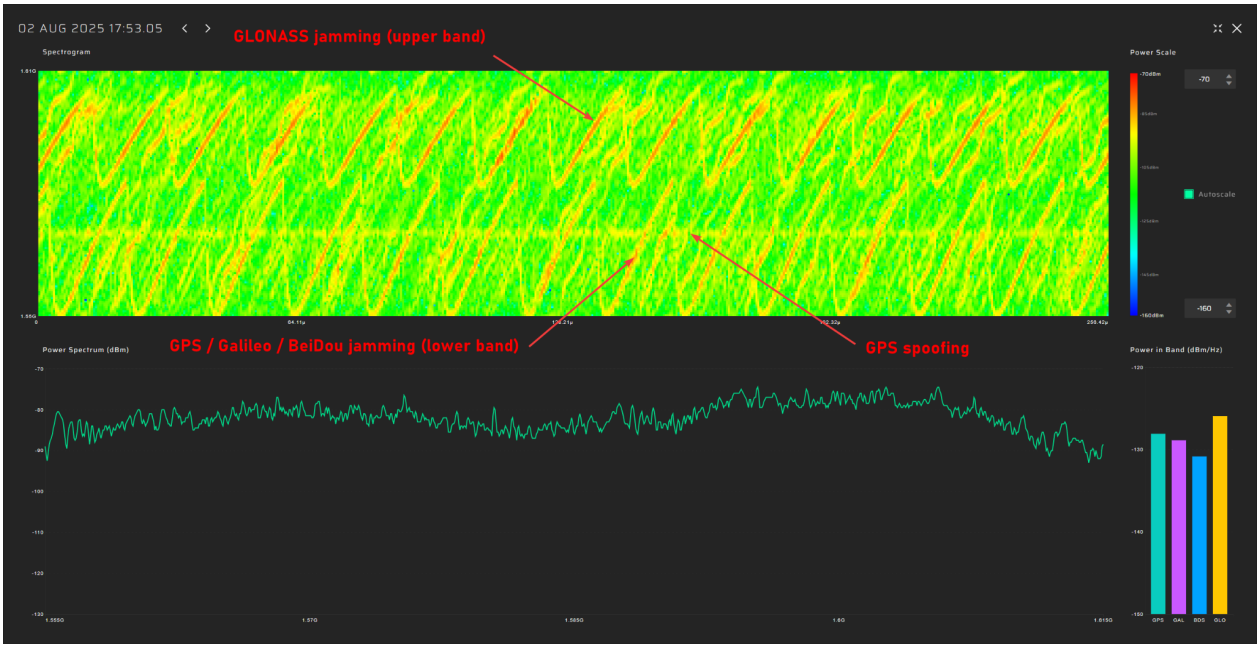
In the next spectrogram, **three distinct interference elements** can be identified:

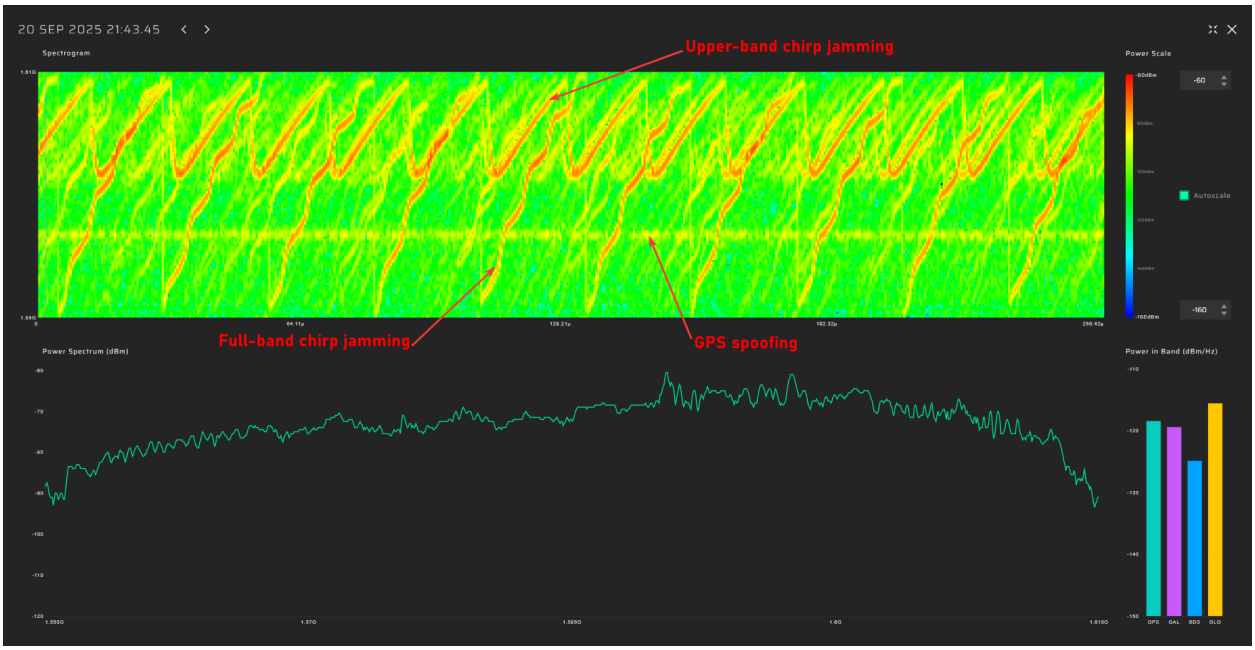
1. **GPS spoofing**, clearly visible and persistent.
2. **Chirp jamming in the lower band**, affecting GPS, Galileo, and BeiDou.
3. **Full-band chirp jamming**, impacting all GNSS constellations including the GLONASS band. The full-band interference shows irregular frequency fluctuations that resemble characteristics of older analog jamming systems.




On the next spectrogram, four interference signatures can be observed:

1. **GPS spoofing**.
2. **Lower-band** chirp jamming for GPS, Galileo, and BeiDou.
3. **Upper-band** chirp jamming specifically in the GLONASS frequency range, with parameters matching the lower-band chirp.
4. Weak traces of a **full-band** jamming signal






**Conclusion**

Across all analyzed spectrograms, the evidence strongly suggests that the interference in the region is generated not by a single transmitter but by **a distributed network of multiple stations**. Several technical indicators support this conclusion:

- Fluctuations in received power correlate with the vessel's heading and antenna orientation, implying multiple arrival directions rather than one dominant source.
- Different interference components appear, disappear, or change power independently, which would be unlikely with a single, continuously operating jammer.
- The observed signals clearly differ in structure: some components exhibit characteristics of older analog systems with parasitic frequency fluctuations, while others show cleaner, more stable spectral patterns indicative of a more modern and technically refined generation method. This diversity suggests heterogeneous equipment rather than a single unified system.
- A notable observation is that the GPS spoofing signal is partially suppressed by concurrent jamming. While such a configuration is technically possible, it is not an efficient design choice...

At the same time, all interference components—spoofing, lower-band chirp jammers, upper-band GLONASS jammers, and full-band analog-like jamming—tend to **activate and cease simultaneously**. This synchronicity indicates that **multiple stations are operating in a coordinated manner under unified tactical control**.

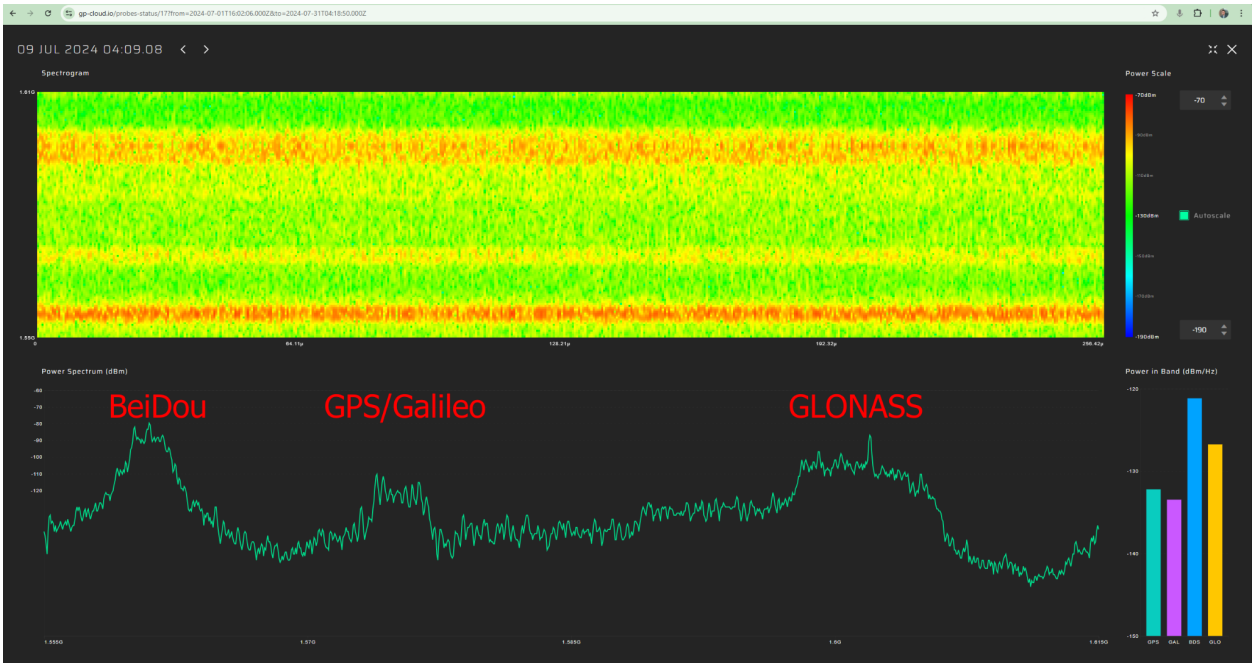
Taken together, these observations point to a **distributed, multi-node interference system**, where several independently operating transmitters—likely of different generations and purposes—are synchronized to work as a single electronic warfare network.

# 6.4 Comparison of Interference Modulation Types Between the Previous and Current Studies

A comparison of the interference signals recorded in our first (coastal) study and those captured in the present shipborne campaign reveals a clear shift in both the modulation types and the technological level of the equipment used.

**Previous Study: High-Quality, Band-Matched Wideband Modulation**

In the first report, the dominant interference source consisted of a high-quality, intentionally engineered three-component wideband signal:



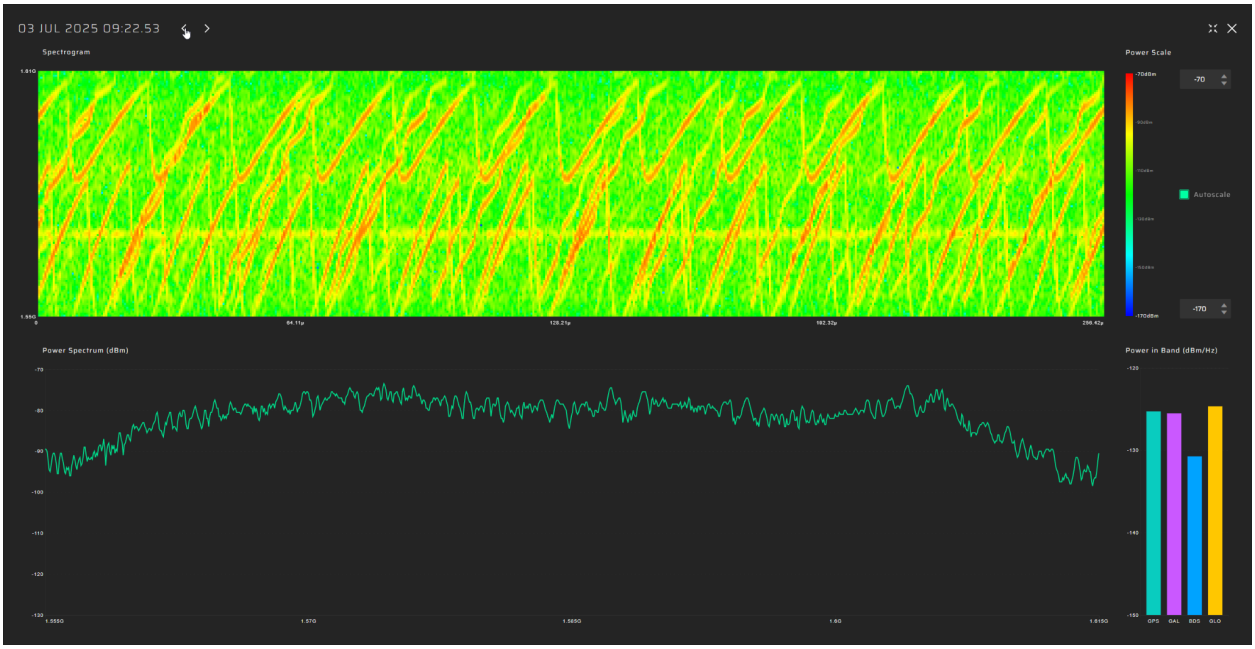

Each component was broadband—likely based on PRN-style modulation—and each precisely matched the bandwidth of individual GNSS constellations:

- a component occupying the GPS/Galileo band,
- a component aligned with BeiDou,
- a component aligned with GLONASS G1.

On spectrograms, the boundaries were sharp and well-defined, indicating a purpose-built, modern interference system carefully designed to maximize jamming efficiency without unnecessary power spillover.

**Current Study: Chirp-Based, Lower-Quality but High-Power Interference**

In contrast, the current campaign reveals interference generated by a very different class of equipment. The primary jamming signals are chirp-modulated, a simpler and generally less efficient modulation type for suppressing GNSS signals. However, despite its lower sophistication, the system compensates with very high spectral power density, enabling it to degrade or fully suppress all constellations across the region:




Moreover, the spectrograms clearly show pronounced parasitic frequency modulations within the wideband jamming signal — a characteristic signature of older, low-stability analog hardware. This strongly suggests that at least part of the jamming infrastructure relies on legacy systems rather than modern, high-quality RF generators.

**Spoofing as the Only Truly "Advanced" Component**

While the jamming elements appear less sophisticated than those observed in the previous study, the current scenario includes a new capability: GPS spoofing.

This marks an upgrade in offensive capability, even if the underlying jamming systems are older.

**However, the combination is technically unusual:**

The full-band jamming signal partially suppresses the spoofing signal. Such self-interference is possible, but not elegant or efficient, and it further supports the conclusion that multiple spatially separated stations are operating simultaneously, not a single unified system.

**Summary**

From a technical perspective, the jamming used in this campaign is less advanced than the high-quality, constellation-matched wideband modulation observed in the previous study. But the overall system is more complex, because it combines:

- multiple chirp jammers from different stations,
- and a persistent GPS spoofing source.

This creates a multi-layer interference environment that is less refined, but significantly more powerful, and operationally impactful than what was recorded previously.

# 7. Most Severe Interference Episode (1–3 July)

The most intense and operationally significant GNSS interference period recorded during the entire campaign occurred between the **evening of 1 June and midday on 3 June**. This interval featured **multiple long-duration and high-power interference events**, with only short gaps between them. Combined together, they created a nearly continuous disruption of GNSS reception.

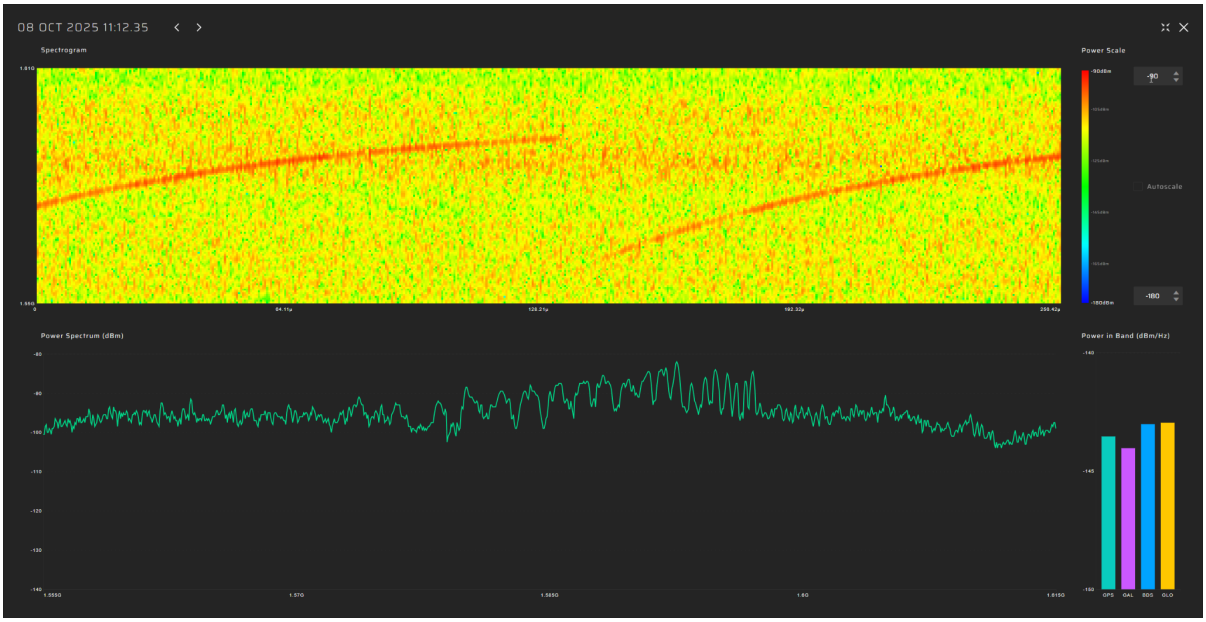

Below is a summary of the main interference phases:

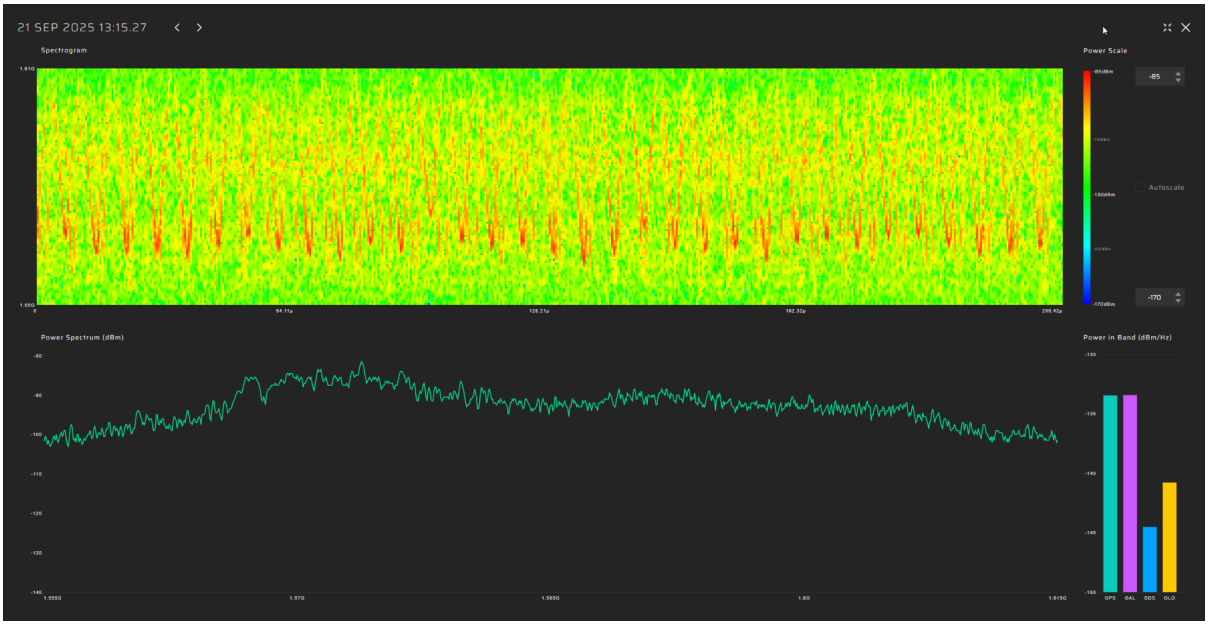
- **1 June, 18:20 → 2 June, 06:00**
  Continuous high-power interference lasting **11 hours 40 minutes**.
- **2 June, 08:00 → 2 June, 19:30**
  Another uninterrupted episode lasting **11 hours 30 minutes**.
- **3 June, 03:18 → 3 June, 11:00**
  A third high-intensity event lasting **7 hours 42 minutes**.

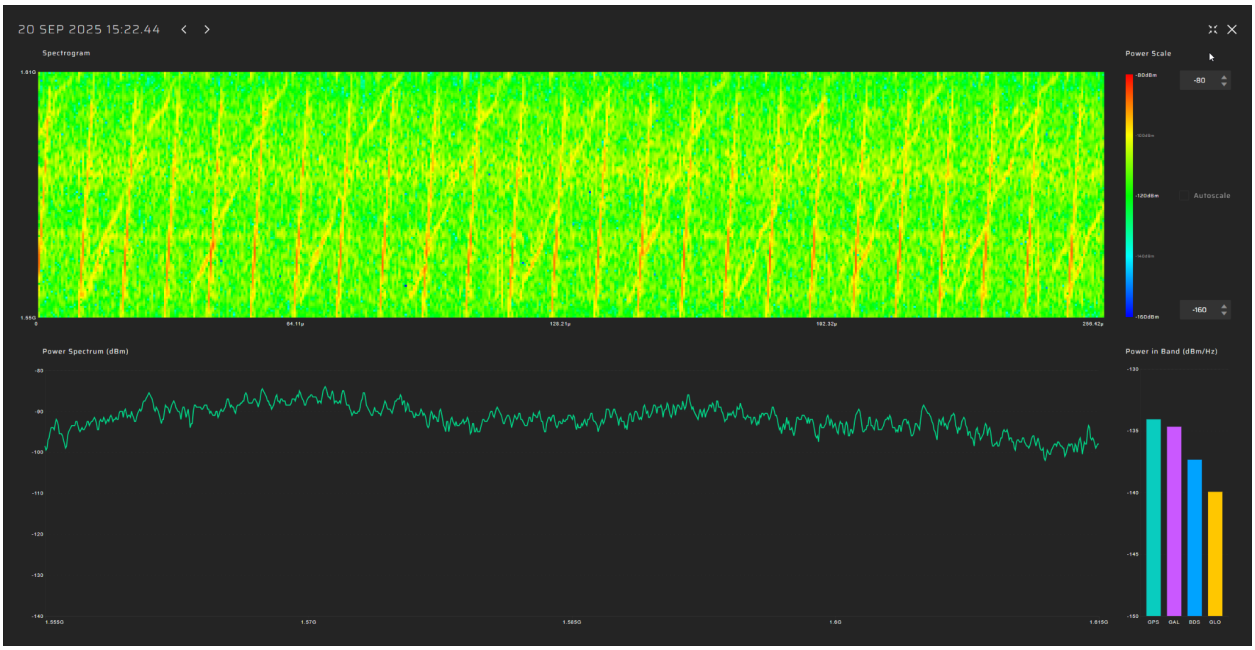
Across these three phases, the combined impact represents **over 30 hours of strong GNSS jamming and spoofing** within a 48-hour window. This was the densest concentration of interference observed during the campaign.

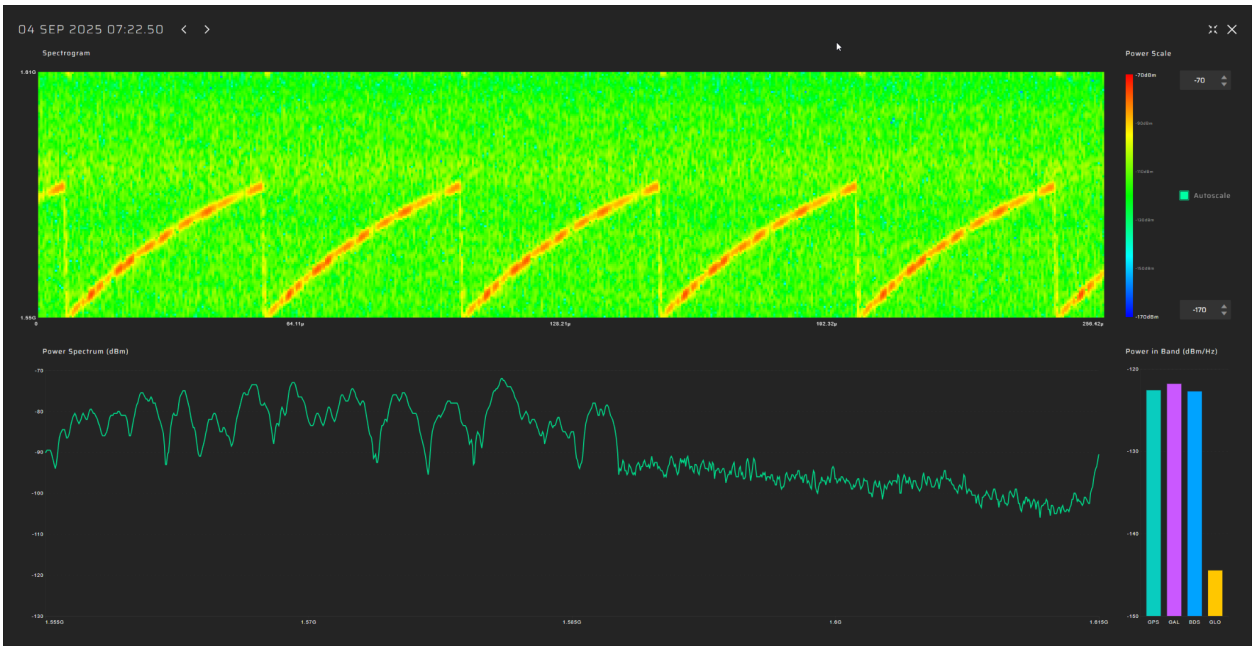
# 8. Automotive Jamming Detected in the Port of Gdańsk

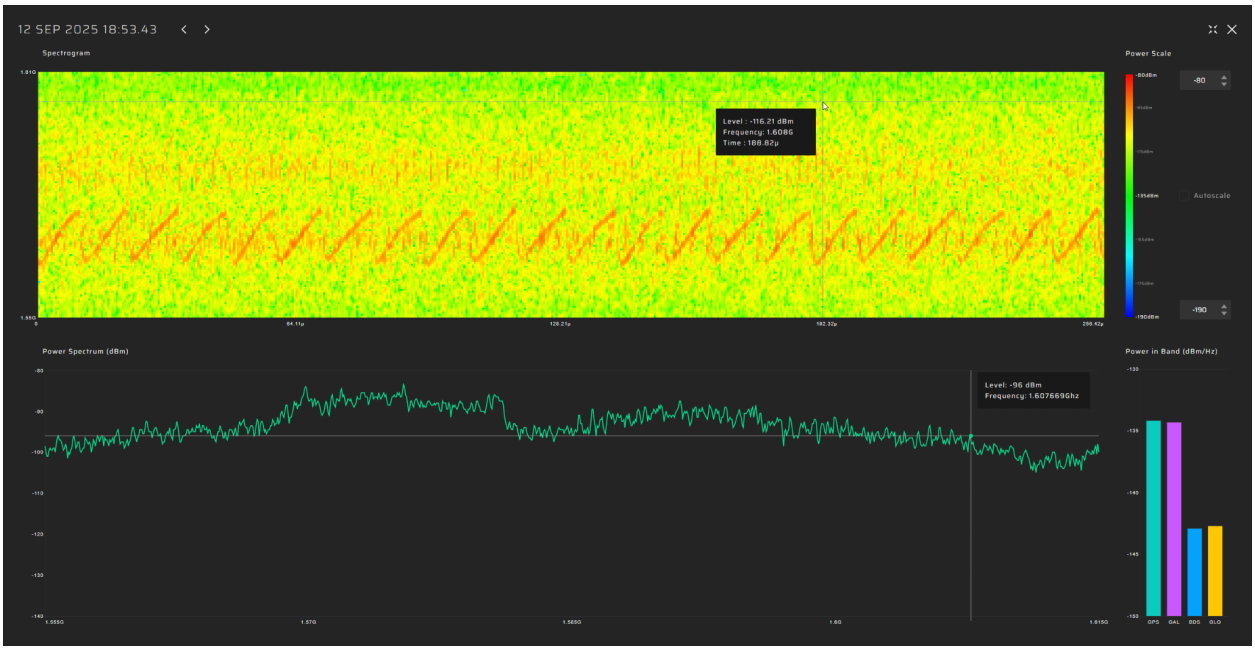
While the vessel was berthed in the Port of Gdańsk, our system repeatedly detected multiple short-duration automotive jamming events, each typically lasting from a few seconds to a few minutes. These signals have characteristic spectral signatures commonly associated with low-power personal GNSS jammers used in civilian vehicles. Below, we present several recorded spectrograms illustrating the variety of these events.

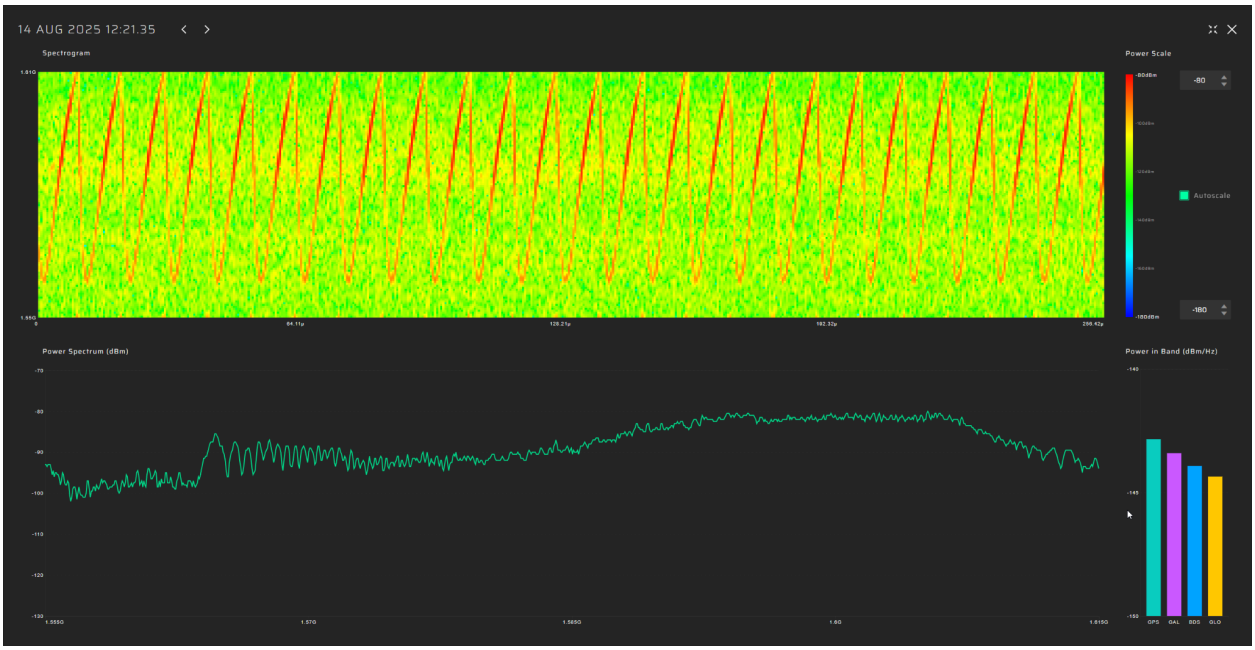


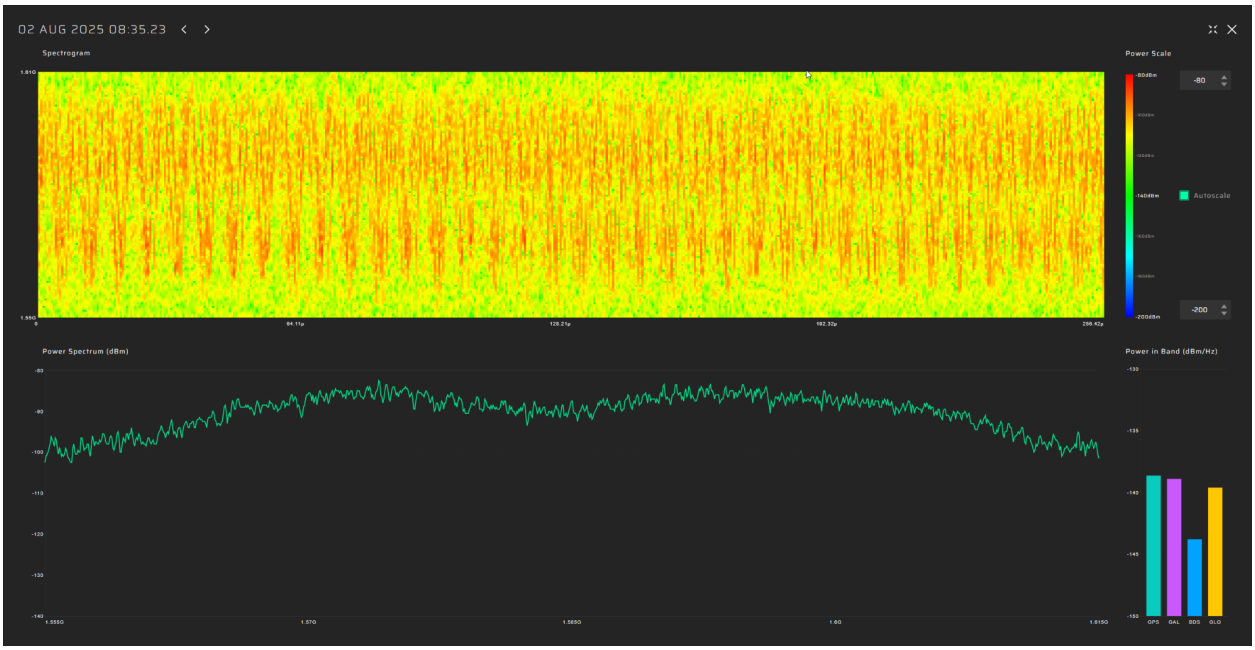



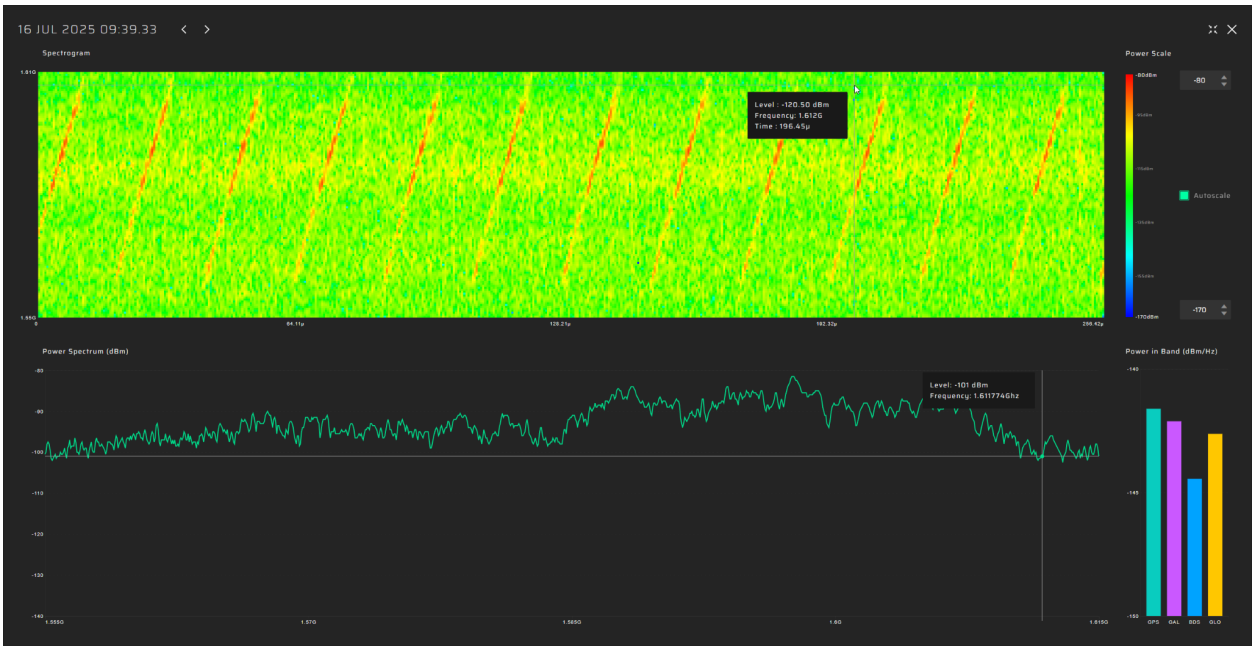


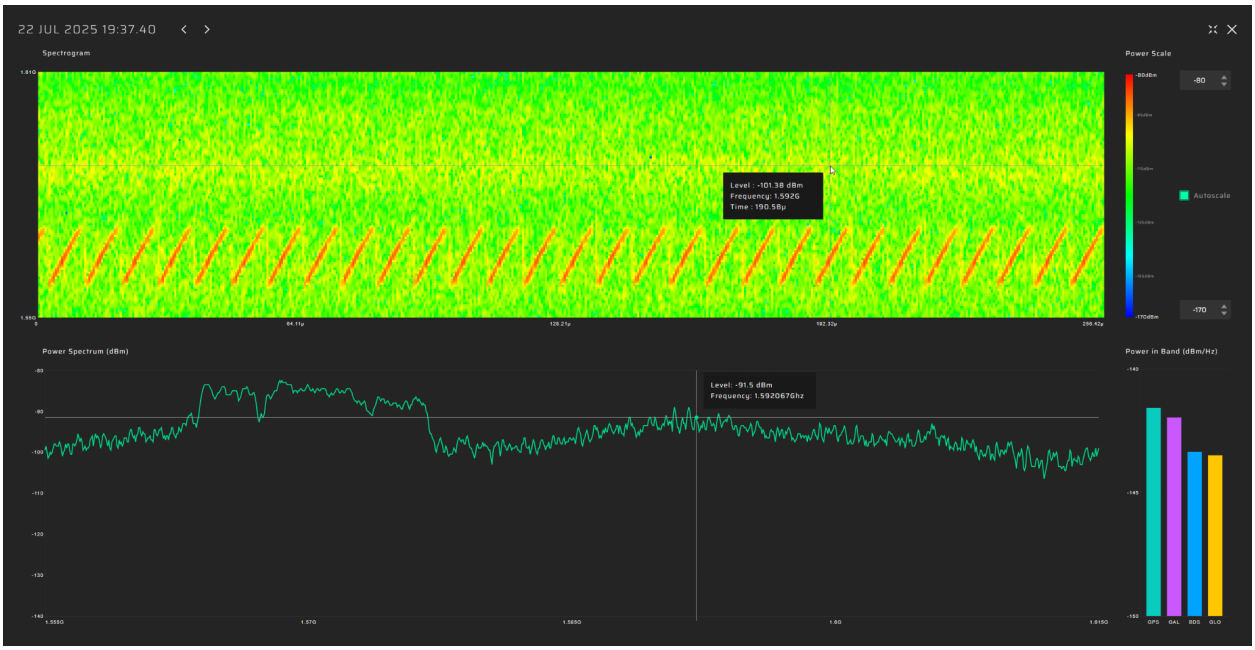







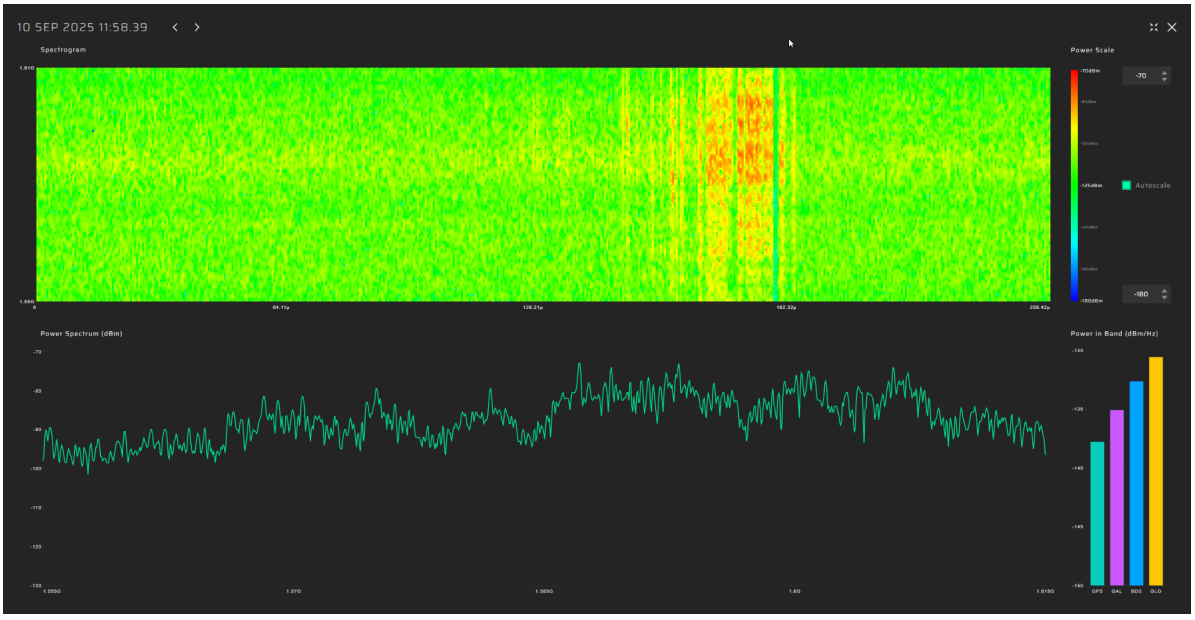



These findings highlight an important point: even in areas without active military electronic warfare systems, vessels may still be exposed to unintentional GNSS interference. Such disruptions can be caused by ordinary vehicles—such as taxis, delivery vans, or long-haul trucks—whose drivers may use illegal GNSS jammers for privacy, route masking, or cargo protection purposes. Although these devices operate at relatively low power, they can still create noticeable interference in harbor areas, temporarily degrading GNSS reception for nearby maritime operations.

# 9. Examples of Industrial Interference

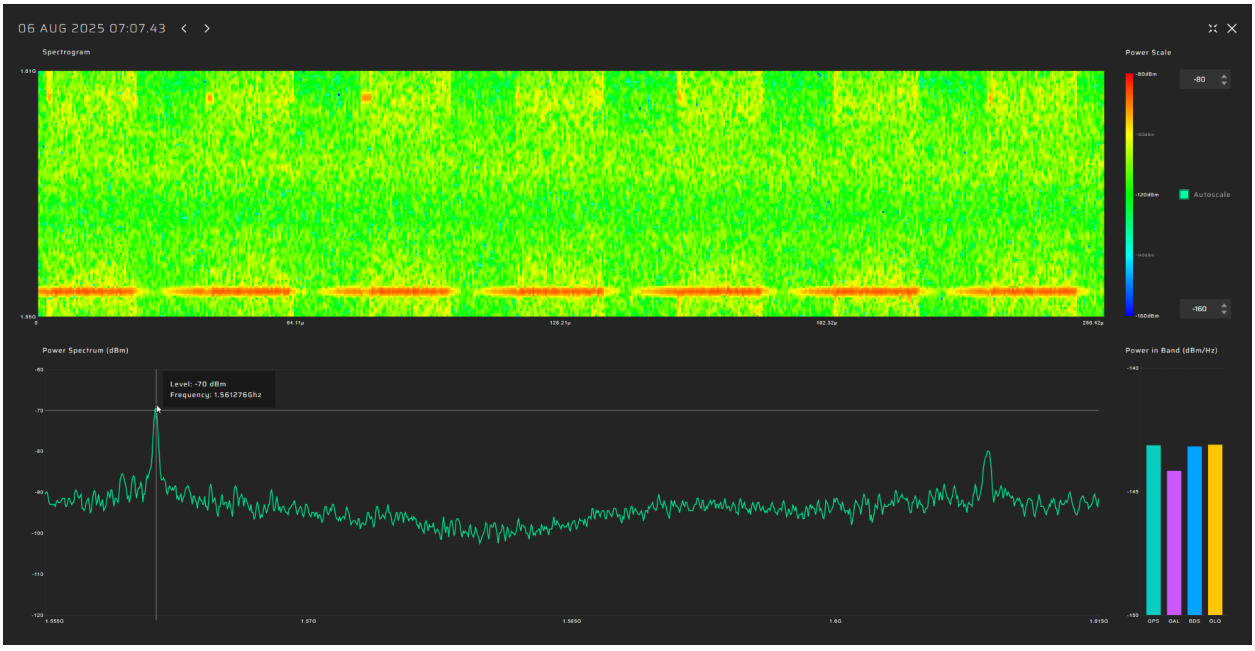
During the campaign, our system also detected several cases of industrial, non-intentional interference, likely originating from electrical or radio-frequency equipment operating near the port area. One such example is shown in the screenshot from GP-Cloud below.


This interference event began on 10 September at 09:29 and ended at 12:13. The spectrogram indicates a broadband noise source that remained active for nearly three hours. The signal exhibits the characteristics of wideband electromagnetic emissions typically produced by malfunctioning industrial devices, or high-power electrical installations:



A similar interference event with the same spectral structure and identical broadband noise characteristics was recorded earlier, on 5 September, beginning at 09:27 and ending at 10:58. The near-identical pattern, duration, and time of day suggest a recurring industrial source, likely associated with equipment that is switched on according to an operational schedule. Although the power level remained too low to affect GNSS performance, the repetition of this signature indicates the presence of a stable, non-intentional RF emission pattern within the port environment.


Short industrial interference event with a clear pattern: **1561 MHz**, **impulse modulation**, **~50 ms repetition period**:



Another industrial-type interference event with a matching broadband noise signature was recorded on **3 September**, starting at **11:03** and ending at **13:45**. Its spectral characteristics were consistent with the events observed on 5 and 10 September, further reinforcing the hypothesis that these disturbances originate from **the same recurring industrial source**, likely operating on a daytime schedule.

# 9. Findings and Conclusion

**Transition From Pure Jamming to Combined Spoofing–Jamming Interference**

In the previous six-month coastal study, 100% of all detected GNSS interference consisted solely of jamming. No spoofing activity was observed at that time.

In the current campaign, however, the interference landscape has fundamentally changed. All major interference events now exhibit a combined structure of GPS spoofing together with multi-constellation jamming.

A notable technical characteristic of this setup is that the jamming component partially suppresses the spoofing signal. While such a configuration is technically possible, it is not an efficient design choice…

**Statistical Summary of Interference Intensity**

The most interference-intensive period of the entire campaign occurred at the very beginning — from late June through July. During this interval, **GNSS availability dropped to 83.2%**, meaning that only 83.2% of the time the system observed no interference and navigation remained fully functional. The total recorded duration of GPS spoofing during this period was 4 days, 5 hours, and 24 minutes, representing the highest spoofing activity level of the entire campaign.

In the following months, the overall intensity of interference gradually decreased, with fewer long-duration episodes and less cumulative impact on GNSS availability.

The single most severe cluster of events occurred between 1 and 3 July, where nearly 30 hours of continuous spoofing were recorded within a 48-hour window. This represents the highest sustained interference level detected during the entire observation period.

**Multi-Emitter Interference Structure Identified from Spectrogram Analysis**

Spectrogram analysis reveals a complex multi-emitter interference environment, consisting of **four distinct signal sources**. Although the jamming components use the same general modulation type (Chirp), they clearly differ in implementation and operate in separate frequency sub-bands. Their synchronous activation suggests coordinated tactical operation, but the observed power fluctuations, varying arrival characteristics, and combined spectrogram patterns show that these emitters are **spatially separated rather than part of a single unified station**.

The four identified interference components are:

1. GPS Spoofing
   A transmitter that generates fake GPS L1 signals designed to imitate real satellite signals.
2. Lower-Band Chirp Jamming (GPS, Galileo, BeiDou)
   A chirp-modulated jammer operating in the lower part of the GNSS L1 band, suppressing GPS, Galileo, and BeiDou.
3. Upper-Band Chirp Jamming (GLONASS G1)
   A second chirp-modulated jamming signal located in the upper L1 sub-band, targeting GLONASS only.
4. Full-Band Analog-Like Jamming Source
   A broadband interference system covering the entire 60 MHz GNSS L1 band. Its fluctuating spectral pattern resembles older, analog-style generation techniques.

Together, these four emitters form a coordinated multi-system interference architecture, operating in unison while originating from multiple spatially distributed stations. Their combined activity explains the layered, fluctuating, and highly complex GNSS interference environment observed during the campaign.

**Evolution of GNSS Interference Modulation**

The comparison between the previous coastal study and the current shipborne measurements shows a clear evolution in how GNSS interference is generated in the region. Earlier, the dominant jamming source was a high-quality, purpose-engineered wideband signal with three clean, constellation-matched components—an indication of modern, deliberately designed equipment. In contrast, the present campaign reveals a shift toward simpler chirp-based jamming. Although these modulation types are technically less advanced, they operate at much higher power levels and are supplemented by a new capability absent in the previous study: **persistent GPS spoofing**. This marks a transition from refined, high-precision jamming to a more complex, multi-emitter environment where chirp jammers, and spoofers operate simultaneously, producing a more powerful and operationally disruptive interference landscape.

### Spatial Gradient of GNSS Interference Strength

The recorded data clearly demonstrates a strong spatial gradient in GNSS interference power. While the signal remains weak inside the Port of Gdańsk, it increases as the vessel moves into open water. At the offshore observation point, the same interference becomes **up to 15 dB stronger**, revealing a substantial rise in power toward the center of the Gdańsk Bay and in the direction of the Kaliningrad region.

This pattern shows that—intentionally or not—the interference system affects maritime traffic far more than coastal infrastructure. The coastal zone experiences only faint traces of the signal, whereas vessels in the Baltic Sea encounter strong, operationally significant disruption.

### Automotive and Industrial Sources

Although the most critical GNSS disruptions during the campaign originated from spoofing–jamming activity offshore, the port environment itself also exhibited recurring non-military interference. Two categories were observed: automotive jamming and industrial RF noise.

### Automotive Jamming

While the vessel was berthed in the Port of Gdańsk, our system repeatedly detected numerous automotive jamming events, each typically lasting from a few seconds to several minutes. Their spectral signatures match those of low-power civilian GNSS jammers commonly used in cars, taxis, delivery vans, or long-haul trucks.

### Industrial interference inside the port area

In addition to mobile jammers, several interference episodes were identified as industrial, non-intentional emissions. These signals included long-duration broadband noise events, sometimes lasting up to several hours. Some noise patterns repeated on different days at nearly identical times, indicating a recurring RF emission from local electrical or industrial equipment.

These findings demonstrate that even in the absence of military activity, vessels operating in busy port areas remain exposed to unintentional GNSS interference generated by civilian vehicles and industrial infrastructure. While far weaker than offshore spoofing and wideband jamming, such disturbances reinforce the importance of continuous GNSS monitoring across both maritime and port environments.