URSI GASS 2026, Kraków, Poland, 15 – 22 August 2026

Characterization of GNSS Interference and its Impact on Air Transport: Poland Case Study

Dariusz Zmysłowski* (1), Jan M. Kelner(1), Jacek Żygólski(2), Olga Kuszpyt(3) and Tomasz Woźniak(3)
(1) Institute of Communications Systems, Faculty of Electronics, Military University of Technology (WAT), Warsaw, Poland
(2) National Radio Frequency Agency (NRFA) Poland, Warsaw, Poland
(3) Polish Air Navigation Services Agency (PANSA), Warsaw, Poland

Abstract

The increasing occurrence of Global Navigation Satellite System (GNSS) interference in Eastern Europe has raised significant concerns regarding the resilience of satellite-based navigation in civil aviation. This paper presents a characterization of GNSS jamming and spoofing phenomena and evaluates their operational impact on air transport based on a case study of Poland. The analysis relies on operational reports collected within the Warsaw Flight Information Region and examines the temporal evolution, spatial distribution, and operational consequences of radio-frequency interference events affecting area navigation and required navigation performance procedures. The results indicate that GNSS interference in Polish airspace has become a persistent, regionally concentrated phenomenon with cross-border characteristics, underscoring the vulnerability of satellite-dependent aviation systems and the need for resilience-oriented operational strategies and contingency measures.

1. Introduction

Over the past several decades, satellite navigation has evolved from a military-oriented capability into a global, safety-critical infrastructure underpinning modern society. Since the initial operational capability of the U.S. Global Positioning System (GPS) in the 1990s, continuous modernization of space, control, and user segments has significantly improved positioning accuracy, integrity, availability, and continuity of service. The proliferation of multi-frequency signals, advanced modulation schemes, and high-sensitivity receivers has enabled centimeter-level positioning in precise applications and robust meter-level performance for mass-market users. Today, global navigation satellite systems (GNSSs) constitute a foundational technology supporting transportation, telecommunications, energy networks, finance, and critical infrastructure synchronization worldwide.

Following the deployment of the American GPS and the Russian GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema) systems, several other global and regional navigation systems have been introduced. The European Union developed Galileo, which reached initial operational capability in 2016 and continues expanding its full operational capacity. China established BeiDou Navigation Satellite System (BDS), progressing from a regional service (BeiDou-1 and BeiDou-2) to a fully global constellation completed in 2020. India deployed the regional Navigation with Indian Constellation (NavIC) system (formerly Indian Regional Navigation Satellite System (IRNSS)), designed to provide positioning services primarily over the Indian subcontinent. Japan implemented Quasi-Zenith Satellite System (QZSS) to enhance GNSS availability and accuracy in urban and mountainous environments in East Asia. Together, these systems form a multi-constellation GNSS environment, increasing redundancy but also complexity in signal processing and spectrum management. In addition, France developed the Doppler Orbitography and Radiopositioning Integrated by Satellite (DORIS) system, primarily designed for precise orbit determination and geodetic applications. Although not a global navigation system in the classical GNSS sense, DORIS has played an important role in satellite positioning and Earth observation missions [1].

GNSS has become a cornerstone of augmentation and performance-based navigation systems, particularly in civil aviation. Both satellite-based augmentation systems (SBASs) and ground-based augmentation systems (GBASs) enhance positioning accuracy and provide the integrity information required for safety-of-life operations. In North America, the Wide Area Augmentation System (WAAS) supports en-route navigation and precision approach procedures, whereas in Europe, the European Geostationary Navigation Overlay Service (EGNOS) [2] enables approaches with vertical guidance, such as localizer performance with vertical (LPV) guidance. Complementing wide-area systems, the Local Area Augmentation System (LAAS), the U.S. implementation of the International Civil Aviation Organization (ICAO)-standardized GBAS, provides high-precision, locally broadcast corrections at individual airports, enabling GBAS landing system (GLS) precision approaches. Together, SBAS and GBAS/LAAS architectures significantly enhance the operational capabilities, availability, and safety of modern air transport, supporting area navigation (RNAV), required navigation performance (RNP), surveillance systems such as Automatic Dependent Surveillance–Broadcast (ADS-B), and other performance-based navigation concepts [3].

Despite its technological maturity, GNSS remains vulnerable to a range of natural and anthropogenic disturbances. Natural phenomena such as ionospheric scintillation, solar flares, and tropospheric anomalies can

degrade signal propagation. However, in recent years, artificial interference (AI) has emerged as a major threat, particularly in the user segment. Intentional jamming, spoofing, and unintentional radio frequency interference can disrupt signal reception, reduce positioning accuracy, or even cause complete service denial. Due to the extremely low received power of GNSS signals at the Earth's surface, even low-power ground-based transmitters may significantly affect receiver performance over wide areas [4].

In this context, the objective of this paper is the characterization of GNSS jamming and the assessment of its impact on air transport, based on a case study of Poland. The analyses presented in this study are based on data provided by the Polish Air Navigation Services Agency (PANSA) [5], derived from reports submitted by civil aviation operators within Polish airspace. The study examines the temporal and spatial characteristics of recorded interference events, evaluates their operational impact on aviation-related GNSS services, and discusses the associated safety implications for the national air traffic management environment.

2. Threats to GNSS

GNSSs operate in a complex space–atmosphere–terrestrial environment that exposes them to both natural and anthropogenic hazards. Natural threats arise primarily from space weather and geophysical processes. Solar storms and associated geomagnetic disturbances may significantly increase ionospheric electron density variability, leading to signal scintillation, phase fluctuations, and temporary loss of lock. Ionospheric irregularities are particularly disruptive at low and high latitudes. Whereas tropospheric delays and multipath propagation introduce additional ranging errors at the user-receiver level. Cosmic radiation can affect satellite electronics and onboard atomic clocks, potentially degrading timing accuracy. Moreover, the space segment remains vulnerable to collisions with space debris or micrometeoroids, and long-term tectonic movements may influence the stability of ground reference stations and geodetic control networks [4].

In summary, natural threats may result in positioning errors, temporary signal outages, degradation of timing precision, and, in extreme cases, physical damage to satellite infrastructure. Variations in signal propagation conditions directly translate into reduced accuracy and integrity, which are critical parameters for safety-of-life applications. Severe space weather events may cause regional or global service degradation, while damage to space assets could affect overall constellation availability [4].

In addition to natural phenomena, GNSS are increasingly exposed to anthropogenic threats, both unintentional and deliberate. Accidental radio frequency interference from terrestrial transmitters may disrupt GNSS reception, particularly because satellite navigation signals are received at very low power levels. Intentional jamming represents a growing concern, as relatively low-power emitters can deny service over considerable areas. Even more sophisticated is spoofing, which involves broadcasting counterfeit GNSS-like signals to mislead receivers and manipulate position or timing solutions. Cyberattacks targeting ground control segments, monitoring networks, or data distribution systems may further compromise system integrity and availability. At the strategic level, the development and potential deployment of anti-satellite (ASAT) weapons introduces the risk of deliberate physical disruption of the space segment [4].

Overall, anthropogenic threats can have severe consequences for transportation systems, financial networks, telecommunications, and critical infrastructure that depend on precise positioning and timing. Jamming and interference may prevent accurate navigation, particularly in aviation and maritime operations, while spoofing can lead to hazardous misguidance of aircraft, vessels, or autonomous platforms. Cyber and kinetic attacks on GNSS infrastructure may result in partial or complete service denial, degradation of quality of service, and significant implications for national security and economic stability [4].

3. Radio Frequency Interference

Jamming and spoofing constitute the most significant intentional threats to GNSS performance at the user level, with jamming representing a form of radio-frequency interference (RFI) and spoofing involving signal deception. Jamming refers to the transmission of radio frequency (RF) signals in GNSS bands with the objective of degrading or completely denying signal reception. It can be broadly classified into several categories. Continuous wave (CW) jamming involves narrowband interference concentrated at a specific frequency, often generated by simple oscillators. Broadband or noise-like jamming spreads energy across a wider portion of the GNSS spectrum, effectively raising the noise floor and reducing the carrier-to-noise density ratio. Swept or chirp jamming dynamically varies frequency over time, affecting multiple channels. More advanced techniques include pulsed jamming and reactive (smart) jamming, where interference is activated only upon detection of GNSS signals. Regardless of technique, the effectiveness of jamming stems from the extremely low received power of GNSS signals at the Earth's surface [6].

Spoofing, in contrast, aims not to deny service but to deceive the receiver by transmitting counterfeit GNSS-like signals. Spoofing can be classified as simplistic (meaconing), in which genuine GNSS signals are delayed and rebroadcast, or as sophisticated generative spoofing, in which entirely fabricated navigation messages are transmitted to manipulate position, velocity, or time solutions. Spoofing attacks may be unsynchronized, causing immediate loss of lock, or carefully synchronized and gradually introduced, allowing seamless takeover of

the receiver's tracking loops. Advanced spoofing may target multi-constellation and multi-frequency receivers, making detection increasingly challenging [7].

From a regulatory perspective, GNSS frequency bands are internationally allocated and protected under the International Telecommunication Union (ITU) framework. These bands are licensed and widely used by both civil and military users worldwide. National and international regulations strictly prohibit the intentional transmission of signals that could interfere with GNSS services, particularly given that satellite navigation signals are inherently low-power when received on the ground. Despite these legal restrictions, commercially available jamming devices, commonly referred to as jammers, are readily available and often marketed as privacy-protection tools [8].

Beyond sporadic interference from personal jammers, there is a category of specialized commercial systems designed for counter-unmanned aircraft system (C-UAS) applications [9], intended to protect sensitive facilities and critical infrastructure. Moreover, GNSS disruption capabilities are integral components of military electronic warfare (EW) systems deployed by armed forces. It is predominantly advanced EW equipment that is currently responsible for large-scale GNSS interference observed in regions such as the Baltic Sea basin, where sustained, geographically extensive disruption events have been reported in recent years.

4. GNSS RFI in Poland

Since February 2022, a significant increase in GNSS RFI has been observed within the Warsaw Flight Information Region (EPWW FIR). The escalation of both jamming and spoofing incidents coincides with the outbreak of the full-scale war in Ukraine. The northern and central parts of Poland have been identified as the areas most affected by GNSS disturbances. The primary external sources of interference are assessed to originate from the territories of the Russian Federation and Belarus, although internally generated disturbances, of both civil and military origin, have also been recorded [10].

The operational data collected by the PANSA [5] form the basis for the analyses presented in this section. The dataset includes reports submitted by civil aircraft crews operating in Polish airspace, as well as internal operational records related to air traffic management. The data demonstrate a clear upward trend in the number of reported GNSS interference events beginning in 2022, with sustained elevated levels throughout 2024 and 2025.

The detailed results, presented in Table 1 and Figure 1, illustrate both the temporal and spatial distribution of interference events [10]. The annual summary for 2025 indicates a continued high frequency of GNSS-related operational reports. Monthly statistics reveal variability in event intensity, with identifiable peaks corresponding to periods of increased regional electromagnetic activity. Spatial analysis shows a concentration of events in specific sectors of the EPWW FIR, particularly in the northern and central regions of the country. Selected terminal maneuvering areas (TMAs), including the Warsaw terminal area, experienced repeated GNSS-related operational occurrences affecting RNAV and RNP procedures.

Table 1. Confirmed TMA RAD events in Poland in 2026 [10].

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
Jamming	1179	827	940	1195	1361	1940	1261	1215	608	494	317	620
Spoofing	282	167	166	170	219	270	179	138	103	83	52	95
CPDLC	2	2	3	5	1	2	2	13	2	-	-	3
Navigation	186	168	145	148	206	290	113	141	65	68	35	72
ADS-B	23	13	12	11	23	10	5	5	2	1	4	8
TCAS	2	-	2	-	-	-	1	1	-	-	-	-
GPWS	25	15	18	23	16	32	8	8	13	4	2	1
Total	**1674**	**1177**	**1268**	**1529**	**1811**	**2512**	**1513**	**1513**	**780**	**646**	**408**	**796**

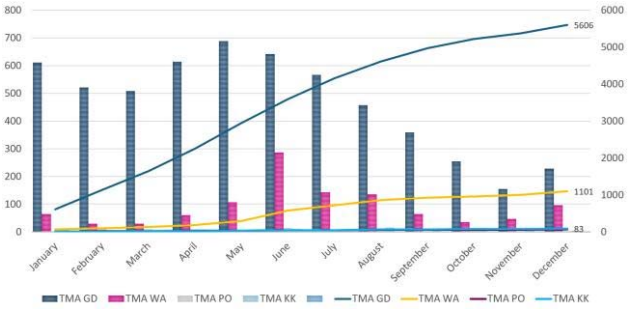


Figure 2. TMA RAD events in Poland in 2026 [10].

Figure 2 presents an example map of GNSS interference over Poland obtained from the open-source monitoring service GPSJAM on 8 January 2026 [11]. This type of visualization illustrates the spatial variability and relative intensity of GNSS interference events, highlighting areas with elevated levels of signal disruption. Such representations are consistent with the concept of situational awareness maps for GNSS jamming and spoofing [12], which are increasingly used to monitor regional interference patterns and to support operational risk assessment in aviation.

The graphical representations further confirm that the interference environment is not uniform but episodic and regionally differentiated. While certain months exhibit moderate reporting levels, others demonstrate sharp increases, suggesting either intensified external interference activity or improved reporting awareness among flight crews. The spatial clustering visible in the figures supports the hypothesis of geographically localized interference sources with cross-border characteristics.

In summary, the results presented in this section confirm that GNSS RFI in Poland constitutes a persistent and operationally relevant phenomenon. The scale, recurrence, and geographic concentration of reported events indicate that interference is not incidental but systematic in nature.

The observed disturbances have direct implications for performance-based navigation operations, cockpit situational awareness, and the resilience of satellite-dependent aviation systems within Polish airspace. The following section discusses the mitigation and contingency measures implemented in response to this evolving threat environment.

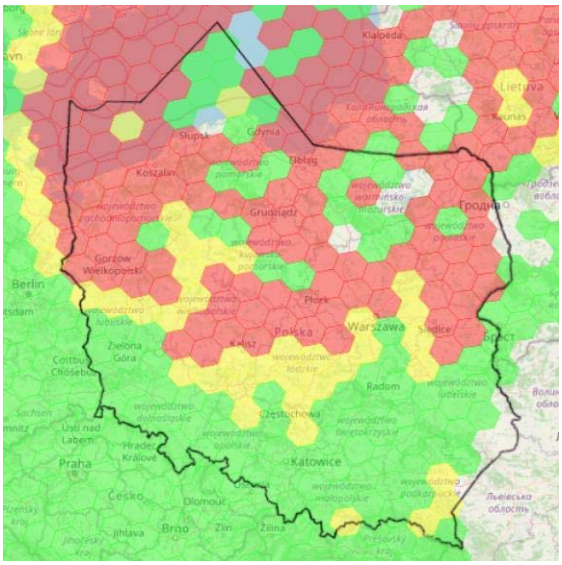


Figure 2. Exemplary GNSS interference map over Poland on 8 Jan. 2026 [11].

5. Summary

This paper has presented a characterization of GNSS jamming and spoofing phenomena and assessed their impact on civil air transport based on the case study of Poland. The analysis, grounded in operational reports from the EPWW FIR, demonstrates that GNSS radio-frequency interference has evolved into a persistent and operationally significant challenge. The temporal variability, spatial concentration of events, and their implications for RNAV and RNP operations confirm that interference is not incidental but systematic in nature, with direct consequences for aviation safety and operational continuity.

The findings highlight the growing need for resilience-oriented air navigation strategies in environments exposed to sustained GNSS disruption. During the conference, additional details will be presented regarding mitigation and contingency measures implemented by the PANSA, illustrating practical approaches to maintaining safety and service continuity under degraded satellite navigation conditions.

6. Acknowledgements

This work was developed within the framework of the grant no. UGB/22-059/2025/WAT, sponsored by the Military University of Technology (WAT), Poland.

References

[1] C. Specht, “Radio navigation systems: Definitions and classifications,” *The Journal of Navigation*, **74**, 5, pp. 945–954, September 2021, doi: 10.1017/S0373463321000369.

[2] A. Felski, A. Nowak, and T. Woźniak, “Accuracy and availability of EGNOS – Results of observations,” *Polish Academy of Sciences, Space Research Centre*, **46**, 3, pp. 111–118, January 2012, doi: 10.2478/v10018-012-0003-0.

[3] F. van Diggelen, *A-GPS: Assisted GPS, GNSS, and SBAS*. in GNSS Technology and Applications Series. Boston, MA, USA: Artech House, 2009.

[4] D. Zmysłowski and J. M. Kelner, “Security threats of satellite navigation systems” in *Cybersecurity – Cooperation vs. information confrontation. Computer science–Law–Management* (in Polish), B. Szafrański, Ed., Warsaw, Poland: Military University of Technology, 2025, pp. 311–325.

[5] “PANSA,” Polish Air Navigation Services Agency. Accessed: Feb. 15, 2026. [Online]. Available: https://www.pansa.pl

[6] D. Zmysłowski, M. Kryk, and J. M. Kelner, “Testing GNSS receiver robustness for jamming,” *Aviation and Security Issues*, **4**, 2, pp. 139-155, December 2023, doi: 10.55676/asi.v4i2.64.

[7] J. Dułowicz, P. Skokowski, and J. M. Kelner, “Survey on intentional interference techniques of GNSS signals and radio links between unmanned aerial vehicle and ground control station,” *TransNav, International Journal on Marine Navigation and Safety od Sea Transportation*, **19**, 3, pp. 931–939, September 2025, doi: 10.12716/1001.19.03.27.

[8] A. Felski, “Methods of improving the jamming resistance of GNSS receiver,” *Annual of Navigation*, **23**, 1, pp. 185–198, 2016, doi: 10.1515/aon-2016-0013.

[9] D. Zmysłowski, P. Skokowski, and J. M. Kelner, “Anti-drone sensors, effectors, and systems – A concise overview,” *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation*, **17**, 2, pp. 455–461, June 2023, doi: 10.12716/1001.17.02.23.

[10] PANSA, “GNSS jamming/spoofing,” Feb. 05, 2026.

[11] “GPSJAM GPS/GNSS Interference Map.” Accessed: Jan. 17, 2026. [Online]. Available: https://gpsjam.obliscence.com/

[12] D. Zmysłowski and J. M. Kelner, “GNSS jamming and spoofing situational awareness maps,” *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation*, (under review) 2026.