

Overview of GNSS Interference Risks in Transport Safety and Resilient Responses [†]

József Orbán 

National Media and Infocommunication Authority, 1133 Budapest, Hungary; jozsef.orban.mba@gmail.com

[†] Presented at the Sustainable Mobility and Transportation Symposium 2025, Győr, Hungary, 16–18 October 2025.

Abstract

Global Navigation Satellite Systems (GNSSs) play a critical role in ensuring the safety of modern transportation across all domains, including aviation, road, rail, and maritime navigation. However, recent years have seen a significant increase in radio frequency interference, including signal masking (jamming) and data deception (spoofing) attacks against GNSSs. These threats can severely compromise human safety, disrupt logistics chains, and undermine essential public services. This study offers a structured holistic overview of the most common forms and impacts of GNSS interference. It also presents practical, resilient solutions to reduce vulnerabilities. Both technological (e.g., redundancy, filtering, alternative navigation) and organizational (e.g., regulation, training, risk assessment) strategies are discussed. The findings highlight that building GNSS resilience is not optional—it is necessary to protect transportation systems that rely on satellite navigation. The summary may be of particular interest to legislators, transport authorities, logistics operators, and policymakers.

Keywords: transport safety; GNSS interference; jamming; spoofing; anti-spoofing; holistic PNT resilience

1. Introduction

A major milestone in the civilian use of GNSSs occurred in 1983, after the Korean Air Flight KAL 007 tragedy. In response, U.S. President Ronald Reagan issued a directive to make the previously military-only Global Positioning System (GPS) available for civilian applications [1]. Since then, Global Navigation Satellite Systems (GNSSs) have become essential to the safe and efficient operation of modern transportation. From aviation and rail safety to maritime navigation and smart road systems, GNSSs play a central role across all modes. However, in recent years, the increasing frequency of radio frequency interference (RFI) has exposed the growing vulnerability of GNSS-based services [2]. These include both signal disruption (jamming) and signal manipulation (spoofing). This paper aims to provide a structured overview of the main threats to GNSSs in transport contexts. It also offers practical strategies to strengthen both resistance (preventing disruption) and resilience (recovering from it) through technological and organizational measures.

2. Objectives, Types, and Phenomena of GNSS Interference

The disruption of satellite navigation systems is a major concern for national spectrum management authorities, whose mission is to ensure the interference-free availability of radio frequency (RF) services. However, interfering with navigation services may, in certain cases, serve national security interests—for example, by preventing or hindering the



Academic Editors:

Szabolcs Kocsis-Szürke, Dániel Csikor
and Boglárka Eisinger Balassa

Published: 10 November 2025

Citation: Orbán, J. Overview of
GNSS Interference Risks in Transport
Safety and Resilient Responses. *Eng.
Proc.* **2025**, *113*, 42. [https://doi.org/
10.3390/engproc2025113042](https://doi.org/10.3390/engproc2025113042)

Copyright: © 2025 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article
distributed under the terms and
conditions of the Creative Commons
Attribution (CC BY) license
([https://creativecommons.org/
licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/)).

navigation of remotely controlled devices used in terrorist operations. One such method involves masking the signals of GNSS satellites with other RF transmissions, such as white noise, or emitting a high-intensity frequency-modulated signal (jamming) [3]. A more sophisticated approach is the transmission of false RF information with greater energy, generating fake position data that misguides or disables the navigating device (spoofing) [4]. Spoofing is a manipulation technique in which the received false GNSS signal appears authentic, thus deceiving the data processing system. A lesser-known variant is replay-based spoofing, in which authentic GNSS signals are amplified and delayed, causing the target device to process outdated time and position information. This can disrupt the functioning of high-precision systems. Although these tools—due to their capability for RF countermeasures—are classified as military-use technologies and are listed on the EU's Common Military List, their manufacturing, possession, and trade are only permitted with non-civilian authorization [5]. Nevertheless, the black market for cheap, widely available jamming devices is rapidly expanding and remains largely unregulated. This situation calls for unified, consistent, and EU-wide regulatory action. The use of such devices endangers all aspects of PNT services: Positioning (P), Navigation (N), and Timing (T). Their impact extends beyond transportation, threatening critical infrastructure protection, as well as telecommunications and banking services [2].

3. Impact of GNSS Interference on Transport Safety

Jamming and spoofing (collectively referred to as interference) pose varying degrees of risk across different transport modes—aviation, rail, road, and maritime—by increasing the likelihood of hazardous situations. In GNSS-based aviation systems, particularly under poor weather conditions, interference can increase pilot workload, raise safety risks, and degrade the precision of maneuvers. In addition to compromising safety, GNSS signal loss in aviation also significantly affects operational efficiency. In rail transport, safety-critical functions such as those of the European Train Control System (ETCS) may be directly impacted [6].

In road transport, interference can lead to various issues, such as incorrect motorway toll calculations, organizing unauthorized cargo routes in freight transport, overcharging passengers through artificially extended taxi routes, or delayed arrival of emergency and disaster response vehicles at accident sites—each of which can exacerbate danger and the extent of damage. The risks are even more pronounced in the case of autonomous vehicles.

In maritime navigation, GNSS interference becomes a major risk factor under poor visibility or in complex traffic situations. In conflict zones and regions under threat of terrorism, GNSS interference is a persistent phenomenon. Its primary aim is often to degrade or disable the accuracy of targeted attacks and is commonly employed as a protective measure—for instance, in the escort of VIP convoys. Understanding these sector-specific impacts necessitates a deeper analysis of positional accuracy requirements across transport modes.

3.1. Risk and Required Positioning Accuracy

In aviation, the adequacy of positioning accuracy is characterized by metrics such as the Navigation Uncertainty Category (NUC) and the Navigation Integrity Category (NIC) or Navigation Accuracy Category—position (NACp). According to the Federal Aviation Administration (FAA), the ADS-B navigation information source is considered reliable when $NIC \geq 7$ (equivalent to 0.2 NM) [7] (p. 16). In contrast, the European Union Aviation Safety Agency (EASA), using a 5 NM separation baseline, considers NIC values between 4 and 6 (0.2–0.6 NM) acceptable [8] (pp. 365–366). However, for precision approaches, the required accuracy must be orders of magnitude higher. Even in the case of

en-route navigation—which requires the lowest level of accuracy—if $NIC < 4$, the GNSS data is classified as unusable, being considered indicative of interference, spoofing, or other system errors.

In the railway sector, the EGNSS-R project (European GNSS Navigation Safety Service for Rail) focuses on managing GNSS system-level integrity. Railway systems—particularly those operating under the ETCS (European Train Control System) and ERTMS (European Rail Traffic Management System) frameworks—comply with the CENELEC EN 50129 standard, using the Safety Integrity Level (SIL) framework. GNSS-based safety-critical applications are generally expected to meet the SIL-4 level, which defines a hazard threshold of less than 10^{-9} dangerous events per hour [9]. In railway safety applications, no simple indicator equivalent to NIC was found. Ensuring GNSS integrity in rail transport therefore requires both SIL-compliant design and multi-sensor monitoring.

In maritime navigation, the IEC 61108 standard series provides detailed specifications for shipborne GNSS receivers (including GPS, Galileo, GLONASS, BeiDou, etc.), covering performance parameters and testing procedures, including interference detection. Although there is no single NIC-like numerical indicator in maritime operations, the systems are capable of detecting GNSS performance degradation. Part 4 of IEC 61108 defines the handling of Differential GNSS (DGNSS) integrity signals: if a faulty correction message is received for more than 10 s, or if the correction exceeds predefined thresholds, the receiver issues a “Don’t use” alert.

In the theoretical assessment of unmanned ground-based navigation, GNSSs remain the exclusive positioning source, given the current state of available onboard navigation systems. While in aviation, an accuracy of approximately 100 m may be acceptable for en-route horizontal positioning, this level of precision is insufficient for safe autonomous ground vehicle navigation—even as indicative information. This aligns with the general conclusion that, in land-based transport, the continuity of GNSS service is a critical safety attribute [10]. The expected positioning accuracy across different modes of transport is summarized in Table 1.

Table 1. Minimum Expected Positioning Accuracy by Mode of Transport (at 95% confidence level).

Mode of Transport	Minimum Expected Accuracy (95% Confidence)
Aviation	~10–15 m (en-route navigation), <1–4 m for precision approach
Rail Transport	~2–3 m (GNSS-based position validation at SIL-4 level)
Maritime Nav.	~10 m (IEC 61108, IMO Res. A.1046(27))
Inland Water Nav.	~5–10 m (typically SBAS/DGNSS-corrected systems)
Unmanned Ground	~0.5–2 m (for safe lane and route keeping by autonomous vehicles)
Drone Delivery	~0.5–2 m (for precision navigation and landing accuracy)

3.2. Advanced Spoofing Techniques and Their Operational Implications

Spoofing refers to the deliberate transmission of counterfeit GNSS signals intended to deceive a receiver by providing manipulated position, navigation, or timing (PNT) data. Spoofing attacks vary in complexity and strategic intent and can be broadly categorized by their underlying technical approach. One of the most elementary spoofing techniques is signal replay, where genuine GNSS signals are recorded, time-delayed, amplified, and retransmitted toward the victim receiver. This method is particularly threatening because it can affect encrypted military-grade PNT signals without the need for decryption—the temporal offset alone can lead to navigational errors or false positioning. More sophisticated spoofing approaches involve the modification and re-synthesis of civilian GNSS signals, enabling the attacker to broadcast precisely crafted position or timing data tailored to mislead the target system. These attacks can simulate the presence of one or multiple satellites, potentially overpowering legitimate signals and taking control of the navigation solution. An especially insidious variant involves a two-stage process: (1) initially transmitting high-power broadband noise (jamming) to cause the receiver to lose satellite lock,

followed by (2) the broadcast of counterfeit GNSS signals at higher power than the genuine signals. In such scenarios, the receiver—upon reacquisition—locks onto the spoofed signals due to their superior signal-to-noise ratio (SNR), resulting in covert capture of the device. Detection and mitigation of spoofing attacks require increasingly sophisticated receiver algorithms and hardware countermeasures, including multi-antenna systems, signal quality monitoring, angle-of-arrival analysis, and timing anomaly detection. As GNSS dependence increases across civil and critical infrastructure domains, these countermeasures are becoming essential components of resilient PNT system architectures.

4. Resistant and Resilient Technological Response Solutions

To ensure the safety and reliability of PNT (Positioning, Navigation, and Timing) services, both theoretical researchers and applied engineers have been working on various countermeasures that reduce the effectiveness of interference—either through resistance or resilience. Resistant solutions refer to methods that improve system robustness by increasing the level of protection, such as hardening signal reception or shielding the antenna from interference. In contrast, resilient solutions are those in which the system detects external manipulation or degradation and adapts its operation accordingly to maintain functional continuity and minimize impact.

4.1. Device-Oriented Resistant and Resilient Technological Solutions

One approach to filtering interference is based on the directional nature of GNSS signals—namely, that useful GNSS signals originate from space, while jamming or spoofing sources typically emanate from ground-based devices. Technological responses may be passive or active, located outside or inside the receiving equipment, and may rely on primary or secondary signal processing techniques. The optimal solution depends on the specific application context and operational constraints. For example, aviation systems may prioritize antenna placement and directional filtering, while autonomous ground vehicles may integrate sensor fusion with inertial navigation systems for redundancy and continuity in degraded GNSS environments.

4.1.1. Reducing Interference at the Antenna Level: Antenna-Based Techniques

Among passive countermeasures, one of the simplest and most effective is antenna shielding against unwanted reception directions. Similarly, elevating the antenna to a higher position can reduce the relative field strength of interfering signals. Polarization-based solutions employ separate reception channels for RHCP (right-hand circular polarization) and LHCP (left-hand circular polarization) signals, thereby improving discrimination between legitimate and spoofed signals. In the case of null-steering fixed antennas, the direction of the expected interference is predetermined, and the antenna can be physically oriented during installation to attenuate that direction. These solutions increase the system's resistance to interference [11].

For high-resilience applications, Controlled Reception Pattern Antennas (CRPAs) are used. These are advanced antenna systems designed for adaptive spatial filtering, employing in-band null forming techniques. The term “in-band” refers to the fact that both the jamming and the desired signal occur in the same frequency band (e.g., GPS L1). CRPAs consist of multiple antenna elements and apply phase shifting to create nulls—points of minimal sensitivity—in the direction of known interference sources.

4.1.2. Receiver-Level Techniques and Signal Processing

Receiver-side techniques that increase resilience include multi-frequency and multi-constellation reception. These approaches enhance robustness by distributing information across different frequency bands (e.g., L1 + L2 + E1 + E5b) and across multiple GNSS

providers (e.g., GPS + Galileo + GLONASS + BeiDou). This diversification helps in both interference avoidance and spoofing resistance. Advanced digital filtering techniques reduce the receiver's vulnerability to noise and jamming. These may involve digital noise suppression, noise-aware transmission path optimization, or spectral analysis. A sudden increase in noise level or an unexpected change in the signal spectrum can trigger automatic alarms, while the receiver may also switch to an optimal demodulation mode based on the detected interference characteristics. Inconsistencies in processed GNSS information—such as abrupt changes in position or time—may also serve as indicators of potential spoofing attempts. Spoofing detection is further enhanced by self-learning systems trained to identify spoofing patterns, providing an additional layer of interference mitigation.

4.1.3. Multi-Sensor Interference Detection and Mitigation

GNSS interference events are often short in duration, offering a theoretical and practical opportunity to apply predictive validation windows based on both positional and temporal parameters. By leveraging auxiliary navigation or timing systems—albeit less accurate—it is possible to define real-time acceptance windows for PNT validation. These secondary systems serve as fallback references in the event of signal disruption. Discrepancies between predicted and real-time GNSS data, based on independent estimation methods, can generate reliable alarms during spoofing attempts. Once a spoofing or jamming incident is detected, the system can deliver tentative PNT data as output. If the output deviates beyond the bounds defined by fallback accuracy, the system triggers an alarm and defaults to the fallback data source. This ensures that even during attacks or system degradation, the maximum error remains within the fallback system's known limits.

4.2. System-Level Resilient Technological Response Solutions

The core objective of holistic PNT resilience is to ensure that the system can continue to deliver reliable position, navigation, and timing (PNT) information even in the presence of GNSS interference, spoofing, multipath propagation, or local signal degradation. The foundational principles of PNT resilience are redundancy, diversity, sensor/data fusion, and autonomy. These principles are best implemented through heterogeneous sensor systems supported by multi-layered data fusion architectures. Redundancy-based systems are not only useful against intentional interference but also serve as mitigation tools in environments where GNSS performance is degraded due to natural or man-made obstructions. High-precision GNSS performance can only be approached through systems that integrate multiple complementary sensors. Before implementing any technological solution, it is essential to define functional requirements and conduct a context-sensitive risk and cost-benefit analysis. Such an analysis helps compare potential solutions not only in terms of investment but also by evaluating the achievable quality of service (QoS) across alternatives. A comprehensive system-level solution must also include the development of local interference detection and alerting networks, which in many cases cannot be replaced by global satellite-based alerting systems, which will be discussed later [12].

4.2.1. Classification of Redundant Systems

Redundant systems can be classified based on their functionality, technology, source independence, application domain, and resilience level:

- Functional classification considers the type of information being replaced or supported, such as positioning, position verification, timing sources, or alternative communication links.

- Technological classification refers to the use of onboard inertial systems (gyroscopes, accelerometers), multisensor fusion (e.g., cameras, lidar), or ground-based infrastructure (e.g., eLoran, Distance Measuring Equipment—DME, radar).
- Source independence classification assesses the system's autonomy from GNSS (e.g., whether it draws data from onboard systems or external sensor networks).
- Application-based classification includes domains such as transportation, critical infrastructure, or communications.
- Resilience level classification evaluates how long the system can maintain an acceptable level of accuracy during GNSS outages.

4.2.2. Comparison of Data Sources by Transport Mode and the Role of Resilience

Even in current road transport systems, the use of automatic navigation systems is of great importance. However, the integration of autonomous ground vehicle traffic (Unmanned Ground Vehicle—UGV) makes their reliable application indispensable. In addition to increasing resistance to GNSS interference, alternative systems providing redundancy are needed. Optical tools are expected to play a significant role in the future of road transport. Various solutions such as camera-based environment recognition and odometry, LiDAR-based mapping, wheel-based odometry, and fallback applications replacing GNSS time services are already becoming widespread. In rail transport, GNSS-based systems play either a primary or secondary role, depending on the country. Due to fixed track operations, odometry based on radar and wheel measurements can provide reliable navigation data. The installation of fallback systems is easier on railways than in aviation, UAV, or road transport, due to space and energy availability.

Distributed systems based on balises, providing absolute position, are being implemented continuously. These offer high reliability but only update the vehicle's position when directly over the balise. GNSS technology has provided a significant boost to air navigation. In the early 2000s, many professional sources predicted the decline of ground-based systems. Performance-Based Navigation (PBN), Required Navigation Performance (RNP), and Satellite-Based Augmentation Systems (SBAS) such as EGNOS and WAAS highlighted the growing dominance of satellite-based navigation in aviation. From a resilience perspective, SBAS is particularly noteworthy. It transmits real-time correction data to GNSS users via geostationary satellites, with the goal of enhancing GNSS accuracy, reliability, and integrity. The SBAS consists of a network of ground stations (RIMS—Ranging and Integrity Monitoring Stations), processing centers (MCC—Master Control Centers), and SBAS geostationary satellites. RIMS monitors GNSS signals, detects orbit and clock errors, and identifies ionospheric disturbances. MCC calculates differential corrections and evaluates GNSS integrity, issuing warning messages if necessary. SBAS satellites then broadcast these corrections to users in a GNSS-compatible format. If a GNSS receiver supports SBAS functionality, it can integrate corrections without requiring additional hardware. Due to the rise of GNSS interference, the role of ground-based distributed DME systems has been reevaluated. These systems offer high levels of RF and cybersecurity resistance. Localization based on signals from multiple ground-based DME stations enables route navigation over land.

For transoceanic navigation, mandating systems like eLoran may be necessary. With ADS-B, the evaluation of NIC/NAC values helps detect GNSS performance degradation. Despite being considered outdated due to GNSS availability, Inertial Navigation Systems (INS) remain a fundamental element of resilient positioning systems. For UAV operations, the challenge is greater due to weight constraints and low altitude. Visual and LiDAR-based geo-positioning and altitude estimation are of particular importance for UAV transport. In maritime transport, vessel size and load capacity allow for the implementation of

multisensor GNSS systems, improving resilience to interference. Radar-assisted navigation, optical environment recognition and identification (e.g., buoys, lighthouses), eLoran, IMU, and AIS all contribute to robust multisensor positioning systems.

5. The Regulatory Dimensions of GNSS Resilience (USA, EU, China, Russia)

The growing vulnerability of transport and critical infrastructure systems that rely on satellite-based positioning has brought GNSS resilience to the forefront of regulatory attention worldwide. Jamming and spoofing are no longer merely technical concerns—they now pose national security, economic, and public service risks. Countries respond to these challenges with markedly different regulatory models.

- The United States is a global leader in regulating GNSS resilience. PNT Executive Order 13905 mandates risk assessment of GNSS-based systems and the implementation of alternative solutions across federal agencies [13]. The FCC's Mandatory Disaster Response Initiative [14] ensures the emergency operability of communication networks. Regulatory enforcement against spectrum interference is supported by software-defined radio (SDR) networks and cyber-based tools.
- The European Union builds GNSS resilience primarily through standardization and regulatory harmonization. Regulation (EU) 2018/1139 governs the integrity of GNSS use in aviation [15], while ETSI EN 303 413 [16] defines technical requirements for receiver robustness. Although EU-level directives are clearly defined, implementation across member states varies significantly due to differing national capacities.
- China builds its resilience strategy on technological autonomy and its national GNSS system, BeiDou [17]. The system uses multiple frequencies and ground-based reference stations, and is supported by legal instruments prohibiting jamming equipment. China also engages in bilateral GNSS dialogues (e.g., with the U.S.) and aligns parts of its policy with ITU guidelines on RNSS protection [18].
- Russia safeguards its GLONASS system [19] through centralized state control and military-civil integration. GNSS use is treated as critical national infrastructure, and the regulation of receiver devices is also centralized. Russia pays particular attention to "reverse spoofing" and covert RF disinformation techniques, while gradually mandating the use of GLONASS-based navigation equipment in various transportation and logistics sectors. Jamming is often officially classified as "defensive," especially near VIP convoys or military installations.

These four countries reflect distinct geopolitical approaches to GNSS resilience. While the USA and EU rely on institutional and standards-based frameworks, China and Russia embed GNSS resilience into their national technology strategies. Future progress will depend on achieving interoperability, strengthening international coordination, and jointly protecting spectrum use—including legal, technical, and security dimensions.

6. Case Study

In May 2025, a technical investigation was launched in response to a reported incident involving a First Person View (FPV) UAV in eastern Hungary. During the flight, the drone became uncontrollable and crashed. Fortunately, there were no injuries, and the damage was limited to the aircraft itself. The operator was an experienced UAV pilot with no prior incidents. The material damage was limited to the destruction of the UAV itself. Based on ADS-B data, GNSS interference was identified at the time and in the area in question. A longer-term analysis of ADS-B data confirmed that recurring GNSS interference had been observed in the region as shown in Figure 1.

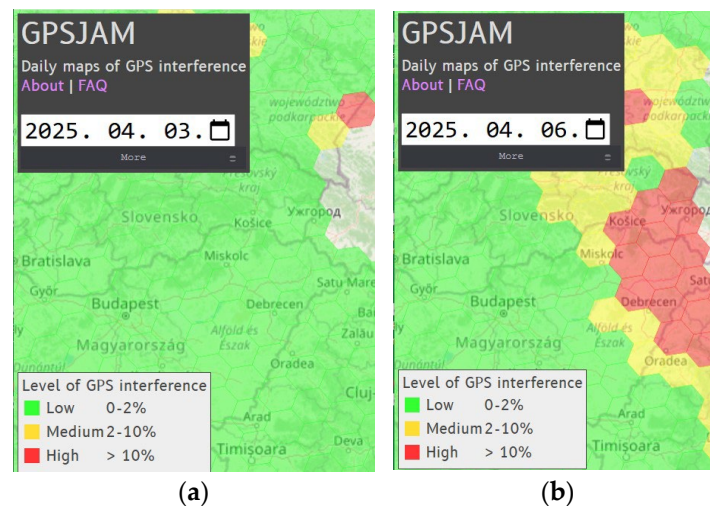


Figure 1. ADS-B-based GNSS jamming maps recorded before and on the day of the incident. The jamming intensity is aligned with the air combat activity reported in the media. (a) Aggregated jamming on 3 April 2025. (b) Aggregated jamming on 6 April 2025.

To prevent future incidents, the competent authority recommended UAV operations in that area be conducted with consideration of the prevailing conditions. Simultaneously, monitoring of the GNSS frequency bands was initiated. The investigation, based on signal pattern analysis, concluded that the interference targeted only the narrow spectral segments carrying data. Direction-finding techniques estimated that the source of interference was located outside the national border. As a result, no immediate mitigation action could be taken to eliminate the interference.

7. Conclusions and Recommendations

GNSS interference is both a technical problem and a societal, economic threat. The three-pillar resilience model shows that future developments must address technical, regulatory, and human factors. Defense cannot rely on technology alone. Strengthening organizational and regulatory resilience is essential. It is recommended that a national GNSS resistance framework be developed, incorporating technological, regulatory, and educational components.

- **Technological Recommendations**

On the technical side, it is important to research and implement new solutions for active and passive multisensor positioning systems. Effective interference detection requires continuous spectrum analysis and the establishment of wide-area SDR-based terrestrial monitoring networks. The creation and regular updating of “heatmaps” showing typical GNSS interference would support overall situational awareness.

- **Regulatory and Cooperative Recommendations**

To ensure the continuity, safety, and security of satellite-based PNT services, it is essential to develop national-level frameworks for the detection, monitoring, and response to GNSS interference. A growing number of countries have deployed independent or regional GNSS interference detection systems operated by governmental, academic, or commercial actors. However, these systems often function in isolation, lacking centralized coordination, data fusion, or real-time response mechanisms. It is therefore recommended that national regulatory authorities establish coordinated GNSS interference monitoring frameworks.

At the international level, this involves coordination between ICAO (aviation), IMO (maritime), ETSI (telecommunications), and at the national level, cooperation among

regulatory authorities, logistics operators, and infrastructure managers. In addition to the existing global ADS-B-based systems, the international integration of local terrestrial detection networks is recommended.

- **Education and Human Factors**

From the human perspective, training should be provided for pilots, train operators, and maritime officers, including reinforcement of knowledge through simulation exercises. Law enforcement personnel should receive additional training to recognize RF-based devices. Awareness should be raised about the illegality of possessing jamming devices, and mandatory actions under national law must be taken. It is also presumed that such devices may support the execution of criminal acts, thereby justifying the implementation of further countermeasures.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data used in the document is based on open source information available on <https://gpsjam.org/> (accessed on 6 April 2025).

Acknowledgments: The author expresses his sincere gratitude to the staff of the NMHH Monitoring Center and to Péter Vári, Deputy Director General of NMHH, for providing valuable consultation opportunities and expert insights during this research.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Reagan, R. Statement on the United States Global Positioning System, 16 September 1983. In *Public Papers of the Presidents of the United States: Ronald Reagan, 1983*; Book II; Office of the Federal Register, National Archives and Records Administration: Washington, DC, USA, 1984; pp. 1250–1251.
2. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. [[CrossRef](#)] [[PubMed](#)]
3. Lubbers, B. GNSS Accuracy Under White Gaussian Noise Jamming. *Eng. Proc.* **2025**, *88*, 26. [[CrossRef](#)]
4. Ji, N.; Rao, Y.; Wang, X.; Zou, D. Advanced GNSS Spoofing Detection: Aggregated Correlation Residue Likelihood Analysis. *Remote Sens.* **2024**, *16*, 2868. [[CrossRef](#)]
5. Westbrook, T. Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe. *Secur. Def. Q.* **2024**, *46*, 104–117. [[CrossRef](#)]
6. Stallo, C.; Salvatori, P.; Coluccia, A.; Capozzi, M.; Gamba, G.; Cianca, E.; Rossi, T.; Di Domenico, S.; Neri, A.; Rispoli, F.; et al. Intelligent Antennas for Mitigating GNSS Jamming & Spoofing Hazards on the ERTMS Train Control. In Proceedings of the ION 2019 Pacific PNT Meeting, Honolulu, HI, USA, 8–11 April 2019; pp. 478–492. [[CrossRef](#)]
7. FAA. *Public ADS-B Performance Report (PAPR) User's Guide*; Flight Standards Service, ADS-B Focus Team, Aircraft Maintenance Division; Technical Report; Avionics Branch: Washington, DC, USA, 2020.
8. European Union Aviation Safety Agency (EASA). *Global Navigation Satellite System Outages and Alterations—Navigation/Surveillance Degradation*; Safety Information Bulletin (SIB) No. 2022-02R3; EASA: Cologne, Germany, 5 July 2024.
9. *EN 50129*; Railway Applications—Communication, Signaling and Processing Systems—Safety Related Electronic Systems for Signaling; European Standard. CENELEC: Brussels, Belgium, 2018.
10. Filip, A.; Rispoli, F. Continuity of GNSS as a Critical Attribute for Safety Applications in Land Transport. *Sci. Rep.* **2024**, *14*, 11742. [[CrossRef](#)] [[PubMed](#)]
11. Park, K.; Seo, J. Single-Antenna-Based GPS Antijamming Method Exploiting Polarization Diversity. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *57*, 919–934. [[CrossRef](#)]
12. Mason, R.; Curry, M.; Jones, J.; Gonzalez, G.; Lee, M.; Lee, J.; Snyder, D. *Analyzing a More Resilient National Positioning, Navigation, and Timing Capability*; RAND Corporation: Santa Monica, CA, USA, 2021. Available online: https://www.rand.org/pubs/research_reports/RR2970.html (accessed on 6 July 2025).

13. *Executive Order 13905: Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services*; Executive Office of the President, Federal Register: Washington, DC, USA, 2020; Volume 85, pp. 9359–9362. Available online: <https://www.transportation.gov/sites/dot.gov/files/2020-02/Executive%20Order%20on%20Strengthening%20National%20Resilience%20through%20Responsible%20Use%20of%20Positioning.pdf> (accessed on 6 August 2025).
14. Federal Communications Commission. 2022 Mandatory Disaster Response Initiative—Improving the Resilience of Wireless Networks. Available online: <https://www.govinfo.gov/content/pkg/FR-2024-03-26/pdf/2024-06092.pdf> (accessed on 6 August 2025).
15. European Parliament and Council. Regulation (EU) 2018/1139 of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. *Off. J. Eur. Union* **2018**, L212, 1–122. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139> (accessed on 6 August 2025).
16. Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) Receivers; Radio Equipment Operating in the 1164 MHz to 1300 MHz and 1559 MHz to 1610 MHz Frequency Bands; Harmonised Standard for Access to Radio Spectrum. Available online: https://www.etsi.org/deliver/etsi_en/303400_303499/303413/01.02.01_60/en_303413v010201p.pdf (accessed on 6 August 2025).
17. Joint Statement on Civil Signal Compatibility and Interoperability Between the Global Positioning System (GPS) and the BeiDou Navigation Satellite System (BDS). Available online: <https://www.gps.gov/news/joint-statement-civil-signal-compatibility-and-interoperability-between-global-positioning> (accessed on 6 August 2025).
18. ITU issues warning on interference with radio navigation satellite service. *ITU News*, 23 August 2022. Available online: <https://www.itu.int/hub/2022/08/warning-harmful-interference-rnss/> (accessed on 6 August 2025).
19. Стандарт эксплуатационных характеристик открытого сервиса (СТЭХОС). Available online: <https://glonass-iac.ru/upload/docs/stehos/stehos.pdf> (accessed on 5 November 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.