

The Impact of GNSS Interference on Aviation

Hannes Alparslan, Cybersecurity expert, explores the challenges of GNSS interference and proposes solutions

Global Navigation Satellite Systems (GNSS) are critical to modern aviation and society at large. GNSS has become an enabler for all facets of daily life and behind all this is accurate Position, Navigation, and Timing (PNT) information provided by satellites in space and sent to GNSS receivers on land, at sea and in the air.

Recent conflicts in Ukraine and the Middle East have highlighted the vulnerabilities and consequences of, and revealed our dependency on GNSS. Stakeholders are increasingly facing the consequences of interference with and disruption of GNSS.

Types of GNSS interference, symptoms and consequences

There are different types of GNSS interference that need to be considered when understanding the challenges and possible solutions.

GNSS jamming is the intentional interference with GNSS signals using radio frequency noise, preventing receivers from accurately determining their location and time.

Spoofing is the act of transmitting fake GNSS signals to deceive receivers into calculating incorrect positions or times. A spoofed receiver indicates a wrong position and time. It calculates a position and time which are incorrect, which is bad; and it is also not able to identify the problem, which is even worse.

GNSS interference can happen during all phases of flight and has far-reaching consequences for aviation. Its effects can be difficult to identify and include differences between ground speed and true air speed, Terrain Awareness Warning System (TAWS) alerts and time shifts.

Not all jamming is illegal as it is used for the protection of high-profile figures, to protect their safety through disguising their exact location.

The FMS screen of an aircraft being GNSS jammed FLIGHTRADAR24

Recent incidents of GNSS interference

Over the past few years, several high-profile incidents have underscored the growing threat of GNSS interference. In 2022, multiple airlines reported navigational disruptions in the Eastern Mediterranean region, affecting flight paths and causing delays. In 2021, flights over the Baltic Sea experienced GNSS signal loss, leading to re-routes and safety concerns. Military aviation has also faced challenges; for instance, during NATO exercises, participants experienced jamming in Northern Europe, leading to operational difficulties and safety concerns.

In April 2024, Finnair announced the suspension of flights to Tartu, Estonia, "until alternative solutions have been established". The airport solely relies on GNSS for approach and landing.

Reports from tracking service GPSJam showed that 46,000 aircraft have shown potential signs of jamming between August, 2023 and March, 2024. 15,000 aircraft had their location spoofed to Beirut Airport, more than 10,000 to Cairo Airport and over 2,000 to Yaroslavl in Russia, although their destinations were somewhere else altogether.

Recommendations and outlook

Reducing the impact of GNSS interference requires a systemic approach involving different elements.

Multi-Layered Navigation

Incorporate diverse navigation systems beyond GNSS, such as inertial navigation systems and terrestrial radio navigation systems.

Some solutions suggest following a so-called hybrid approach where GNSS information is augmented with other technologies like an atomic clock to provide accurate timing in case GNSS is disrupted.

Other navigation approaches investigate downward looking imaging technologies that scan the terrain and compare that information with available mapping information to determine the current position and trajectory of the aircraft.

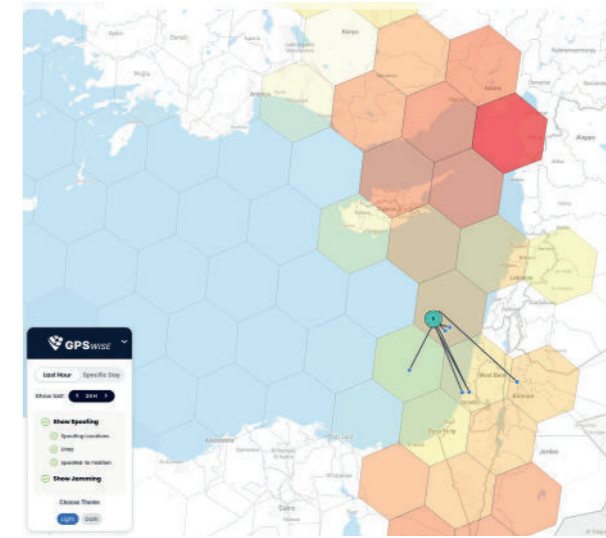
Invest in Technology

Research and development of new technologies to counteract jamming and spoofing is ongoing, and some solutions are in the pipeline. For the time being such solutions merely cater to military use cases however, derivatives may over time also find their way into commercial usage.

Some companies and researchers also invest significant resources into jamming and spoofing resistant equipment.

Cooperation

International collaboration and information sharing can significantly contribute to situational awareness and enable a more proactive approach to GNSS interference. Some European Union institutions and organisations, often in collaboration with representatives from the military, have already established adequate forums facilitating the exchange of information, experiences and solutions.



ABOVE: SKAI GPSWise's GNSS interference report over the Eastern Mediterranean Sea SKAI DATA SERVICES

Collaboration on best practices and standards can be another critical enabler not only reducing financial burden on operators but also ensuring a more coherent approach to GNSS interference beyond national borders. In 2023, the International Civil Aviation Organisation (ICAO) through its Navigation Systems Panel (NSP) adopted new standards permitting the combined leverage signals from up to four GNSS constellations simultaneously.

Training and Awareness

Aircraft can fly safely even if denied GNSS access, but such a situation leads to an increased workload on the flight deck. To enable flight crew to be better prepared, widespread awareness campaigns should be conducted about such incidents and how those can best be identified.

Ideally, this is accompanied by training and updated procedures enabling appropriate handling of such situations to reduce the impact of GNSS interference on Flight Operations.

The aviation industry must prioritise resilience and adaptability. By addressing the challenges of GNSS interference head-on, stakeholders can safeguard the skies and ensure continued progress and safety in aviation operations. The ongoing investment in resilient technologies and international cooperation will be key to overcoming these challenges and maintaining the integrity of global aviation systems.

A longer version of this article is available on Global Airspace Radar website at <https://globalairspace.com/default/the-impacts-of-gps-jamming-and-spoofing-on-aviation/>



HANNES ALPARSLAN
Hannes Alparslan is an expert in system architecture and cybersecurity. He worked for Austro Control, the European Defence Agency, and is a teacher at EUROCAE.