GPS interference in geopolitical conflict zones

In an increasingly connected world, maritime navigation has become heavily reliant on the Global Positioning System (GPS). This omnipresent technology provides pinpoint accuracy for vessels. However, a growing threat is also emerging - GPS interference and disruption.

Published 22 July 2025

Far from being a theoretical concern, recent incidents in geopolitical conflict zones have underscored the very real and immediate dangers posed by compromised global navigational satellite systems (GNSS).

Building on claims Gard has handled stemming from GNSS disruption in such regions, this article looks at the growing problem of GNSS interference at sea, exploring its manifestations, the risks it poses to maritime safety, and the need for countermeasures.

There are several Global Navigation Satellite Systems (GNSS) in operation, including China's BeiDou (BDS), Europe's Galileo, Russia's GLONASS, the USA's GPS, India's IRNSS, and Japan's QZSS. Due to US GPS's extensive history, established infrastructure, and widespread application, this article will focus on GPS disruption.

Case Studies on the multifaceted impacts of GPS disruption in conflict zones

Case study 1

en-US

Case study 2

en-US

These case studies collectively highlight several key points. Firstly, they illustrate that GPS interference is a real and present danger, particularly in regions of geopolitical tension, rendering primary navigation systems unreliable. Secondly, these disruptions force seafarers to make critical "go/no-go" decisions, with contrasting choices and outcomes observed in the two cases. Thirdly, the first case tragically underscores the dangers of trusting an Estimated Position (EP) derived from ECDIS when underlying GPS data is compromised, and no conspicuous objects are in the vicinity for visual cross-referencing. Finally, the successful use of LRIT in the first incident, operating on a different satellite communication frequency than GPS, emphasizes the vital role of tracking systems other than GPS in confirming the vessel's actual location. We will now elaborate on some of these factors.

GPS interference

Typical causes of GPS signal interference

GPS disruptions are caused by a mixture of factors: natural events like solar flares, equipment problems such as receiver or antenna malfunctions, and, increasingly, deliberate interference. Deliberate interference has become a feature of modern conflict and geopolitical tensions. In areas experiencing conflict, strategic rivalry, or heightened tensions, States are actively using GPS interference for reasons such as –

- Denying adversaries access to crucial positioning data;
- Protecting critical infrastructure from potential attacks; and
- Obscuring military movements.

These deliberate operations frequently impact civilian activities, particularly maritime navigation in nearby sea lanes. Recent instances where GPS interference served as a defensive measure against drone and missile threats targeting critical infrastructure include the Israeli coast and the Red Sea during the Israel-Hamas conflict as well as the Persian Gulf and Arabian Gulf

As illustrated in the map below, a growing number of regions globally have experienced GNSS interference throughout 2025, highlighting the widespread nature of this challenge.

Source: Norma Cyber.
Note: Geographical boundaries of GNSS interference are not precisely depicted.

Beyond state actors, criminals are increasingly using GPS jammers for their illicit activities. These devices are employed to disable tracking systems on trucks, containers, and vessels, particularly in and around ports and logistics hubs, thereby facilitating theft and other crimes. This trend underscores the evolving tactics of organized crime groups in the face of widespread GPS tracking.

GPS jamming vs. spoofing

Two terms often used interchangeably but with distinct meanings are GPS jamming and GPS spoofing. GPS jamming is the act of blocking or interfering with legitimate GPS signals by overwhelming them with stronger, unauthorized radio signals. Think of it as trying to have a conversation in a very noisy room – the noise makes it impossible to hear what the other person is saying. GPS spoofing is the act of transmitting false GPS signals designed to deceive a receiver into calculating an incorrect position, velocity, or time. Instead of blocking the signal, a spoofer imitates a legitimate GPS signal, making the vessel's receiver believe it's real. The GPS display will show a position, but it will be inaccurate, potentially by a significant margin. Derived speed and course information will also be incorrect. Below is a summary of key differences:

Feature	GPS jamming	GPS spoofing
Effect	Blocks or denies GPS signals	Deceives with false GPS signals
Result	Loss of GPS signal/No position fix	Incorrect, but seemingly valid, position fix
Indication (discussed below)	"No Fix," "Acquiring Satellites"	Illogical position shifts, mismatch with other aids

GPS disruption: alarms and indications

Recognizing the signs of GPS disruption

Mariners must maintain heightened attention and awareness for signs of GPS disruption, as numerous onboard systems — including ECDIS, Radar/ARPA, Gyro compass, course recorder, and the autopilot — are heavily reliant on the GPS feed and will likely be impacted by any disruption. Depending on whether the disruption is caused by jamming or spoofing, the tell-tale signs can vary from clear audible or visual alarms to no alarms at all. While specific indications for GPS disruption can vary between equipment and manufacturers, examples shared by Anglo-Eastern's Maritime Training Center, Delhi, India, highlight key signs mariners can watch out for.

When GPS jamming occurs, mariners may observe unusually high HDOP values, e.g., greater than '4' indicating unreliable accuracy, RAIM alerts entering caution or unsafe modes, or elevated Signal-to-Noise Ratio (SNR) values. On ECDIS, jamming can trigger sensor failure alarms, potentially leading to a switch to backup sensors or dead reckoning and may even freeze the chart display if no secondary source is defined. Conversely, spoofing presents a more deceptive threat as the GPS receiver might report an erroneous but seemingly valid position, often without RAIM detection. In such spoofing scenarios, ECDIS can display incorrect positions, and radar/ARPA systems, when GPS-fed, will show erroneous data, while gyro compasses may enter an alarm state if relying on GPS for drift stabilization. It's important to note that a comprehensive list of every possible indication across all bridge equipment is beyond the scope of this discussion.

Alarm fatigue and sensory overload

A significant challenge during GPS signal loss is alarm fatigue. The disruption or loss of GPS signal often triggers numerous simultaneous alarms across the bridge, leading to a sensory overload that can be both disconcerting and distracting for the crew. Effectively managing these alarms and prioritizing critical information is essential to maintain situational awareness and ensure safe navigation.

Beyond Alarms: Covert GPS Failures

There are also situations where no alarms are triggered, making detection much harder. For example, the Australian Transport Safety Bureau reviewed a near-grounding incident involving a vessel navigating the Great Barrier Reef. In this case, a malfunctioning GPS unit (due to an antenna fault) fed incorrect positional data to the ECDIS, radars, and other bridge equipment. Because the ship's position wasn't being monitored through other means and no alarms were activated, the inaccurate GPS data and the vessel's deviation from its planned course went unnoticed by the crew, pilot, and even Vessel Traffic Services (VTS). While not linked to jamming or spoofing, such cases underscore the dangers of unaddressed GPS anomalies, whether from technical faults or external interference. They highlight the inherent risks of relying solely on a single source of navigational data, even when it appears functional, and emphasize the importance of crew training in recognizing and responding to these events.

Responding to GPS disruption

Technical mitigating measures

For detailed guidance on effective mitigating measures in such scenarios, owners and the bridge watchkeepers are encouraged to refer to Intertanko's ' Jamming and Spoofing of Global Navigation Satellite Systems '. This comprehensive resource outlines key strategies such as switching to a secondary receiver different from GPS (if available), employing parallel indexing, utilizing RADAR overlay on ECDIS, and manual position plotting on ECDIS. It's crucial to emphasize that once a GPS interference alarm is triggered, mariners must identify its root cause instead of simply silencing or deactivating it.

Regarding manual position plotting, the varying levels of user-friendliness of ECDIS remains a significant concern. As noted by Anglo-Eastern's Maritime Training Center, Delhi, India, some units allow a manual position fix in just three clicks, while others demand up to thirteen; a difference that can foster negative user biases and deter effective equipment utilization. It is crucial to note that while manual position plotting by range and bearing is possible near conspicuous landmarks, it may not be feasible when a vessel is far from land, navigating a flat coastline, or lacks discernible objects.

Operational decisions and voyage continuation

Beyond the technical measures, vital operational decisions become critical, such as

• reducing speed, which not only allows more time for assessment but also significantly lessens potential damage during an incident like grounding,
• increasing bridge manning, and
• making informed decisions on whether to proceed with the voyage.

This critical go/no-go decision should be guided by a comprehensive set of considerations, ideally integrated into the vessel's GPS disruption response plan. Such factors include:

• the complexity of the passage,
• room to manoeuver,
• the availability and capability of pilots or local tugs for assistance,
• the reliability of buoys and fairway markings,
• the presence of safe anchoring points along the route,
• the density of traffic,
• effectiveness of Vessel Traffic Service (VTS) management,
• visibility, and
• the geographic extent of the GPS disruption.

Contractual concerns

As our second case study above illustrates, contractual disputes can readily arise between owners and charterers due to GNSS disruption. The simple fact is that GNSS disruptions will often have an adverse impact on the operation of a vessel. In some cases, forcing speed reductions, causing erroneous deviations from the intended route, or even necessitating the interruption/suspension of the voyage until navigation becomes safe again. In all these scenarios, there will be a loss of time, and potentially significant commercial losses, such as a vessel arriving outside of a laycan or missing a space in the berthing line-up. More serious claims can also emerge, especially if the vessel runs aground, as highlighted in our first case study.

Vessels, of course, do not navigate by GPS alone; and while GPS has undoubtedly enhanced navigation safety, ships successfully sailed without it for hundreds of years. Therefore, a primary consideration is whether a disruption to GPS signals would, in fact, entitle a Master to change speed, course, or intentions. The answer, as explained, is that such actions can certainly be justified. The Master holds an overriding duty to ensure the safety of the crew, cargo, the environment, and the ship itself, all of which may necessitate the adjustment of course plans or voyage suspension. Each case must of course depend on its facts, but if the Master reasonably adjusts speed or suspends a passage because conditions render navigation unsafe without reliable access to GPS, the vessel will typically remain on hire, and the suspension would not be considered a breach of contractual service.

The critical question in such cases is whether the Master's decision to reduce speed, suspend passage, or deviate was genuinely justified by the circumstances, or should he have proceeded as the charterers ordered, despite the GPS disruption? This hinges on the specific facts, including passage complexity, availability of anchorage areas, traffic density, visibility, proximity to hazards, and the presence of clear geographic markers for position fixes. While arbitrators may have some sympathy for Masters tasked with operating large vessels without a key navigational tool, they will also expect Masters to be capable of navigating effectively using alternative methods where prevailing conditions permit. This assessment will be highly dependent on the unique details of each incident.

Insurance implications

There is no explicit exclusion in the International Group Poolable Club cover for losses due to cyber risks providing losses fall within the relevant Club Rules. It is common for Marine risk policies to incorporate Cyber Exclusions, e.g. LMA5403 (Marine Cyber Endorsement) or Clause 380 (Institute Cyber Attack Exclusion Clause). These exclusions will typically exclude Malicious Cyber-attacks. However, due to a lack of clear legal precedent, determining if GNSS interference damage is caught by Cyber Exclusions will be highly dependent on the unique facts of each individual case.

For any cover-related queries, clients are advised to reach out to Gard underwriters.

Key recommendations

Preparedness

• Ensure mariners are thoroughly trained in detecting GNSS disruption, understand alarm triggers, and execute appropriate responses. It is worth noting that there have been proposals to the IMO for a new competence on navigating in a GNSS impacted environment, for example by Intertanko (ref. HTW10/6/6, 2023).
• It is important for owners and managers to consult equipment manufacturers for advice regarding indications on their equipment in the event of GPS disruption.
• Develop and implement clear, concise and practical procedures for mariners to follow during GNSS disruptions. These procedures should also offer guidance on voyage go/no-go decisions, and the necessary considerations. It is crucial to recognize that loss of or manipulation of position data would also form part of vessel's cyber security and risk management.

Bolstering onboard systems and resilience

• Consider equipping vessels with secondary satellite receivers, other than GPS, that are recognized by the IMO as part of the Worldwide Radio Navigation System for both ocean waters and harbour approaches. Ensure all such equipment is reflected in relevant ships' certificates. Additionally, owners can also consider backup systems like eLORAN, acknowledging their limited global coverage.
• Consideration can be given to equip vessels with counter-jamming solutions such as receiver filtering, IMUs, CRPAs, and multi-frequency GNSS. For spoofing protection, owners should ensure their equipment actively monitors GNSS Key Performance Indicators (KPIs) and incorporates anti-spoofing features. The implementation of CRPA antennas or centralized GNSS data distribution can also be explored, based on vessel configuration and budget, as has also been recommended in Intertanko's 'Jamming and Spoofing of Global Navigation Satellite Systems '.

Communication, reporting, and operational decisions

• Making a critical go/no-go decision should be guided by a comprehensive set of considerations, ideally integrated into the vessel's GPS disruption response plan.
• Reporting* of all suspected GNSS disruptions to relevant authorities and organizations to aid wider situational awareness and warnings.
• Proactive Owner-Charterer dialogue if the vessel is heading towards a region when GNSS disruption can be experienced.

References

• Joint statement by IMO, ITU and ICAO on'Protection of the radio navigation satellite service from harmful interference'
• Intertanko'sJamming and Spoofing of Global Navigation Satellite Systems (GNSS)
• Satellite navigation service interference in Finland
• TheAustralian Transport Safety Bureau's investigation report of a near grounding incident caused by GPS malfunction
• Gard article:GPS interference and jamming on the increase
• Gard case study:LP Case study - Grounding due to GPS jamming

We would like to thank Capt. Naveen Sharma at Anglo-Eastern's Maritime Training Centre (AEMTC), Delhi, India and Arne Asplem of Norma Cyber for their assistance in this insight.

**Since 2020, Gard has been a member of NORMA Cyber, a non-profit cyber security service company established by Norwegian shipowners and supported by the Norwegian Coastal Administration in their role as sectorial response function for cybersecurity within the Norwegian maritime sector. NORMA Cyber welcomes all voluntary reporting of cyber incidents from Gard's Members and will act as an advisory body to Gard when needed during an incident and crisis management, as well as contribute to warnings and reports.*