IMPACTS OF GNSS INTERFERENCE ON MARITIME SAFETY

A special report by the RIN Maritime GNSS Interference Working Group

Digital Report Published January 2026

Contents

Foreword: Captain James Taylor OBE FRIN

Fellow and Trustee
of the Royal Institute
of Navigation

The concept is utterly brilliant. A network of satellites, 20,000 kilometres above the Earth's surface, emitting weak but incredibly accurate time signals in an agreed frequency band, providing position, navigation and timing (PNT) to users worldwide, be it GPS, then GLONASS, BEIDOU or GALILEO. The removal of selective availability from GPS made it truly, "America's gift to the World," a gift with global access and global use, leading to a global dependency.

Yet the very nature of the constellation makes it vulnerable not only to the forces of nature, the solar winds, but to malevolent forces, be they individual or state-sponsored, in the form of jamming or spoofing. Despite measures to improve resistance to jamming, spoofing and other harassment measures, the threat is real and growing. And this threat is not only to positioning and navigation; it is to every part of every transport and navigation means and to every part of national infrastructure where timing is derived from space-based timing signals. Whilst this report deals essentially with maritime PNT, there is a read-across to every transport means, by land, air, sea or space and to every management system wherever located, requiring precision timing for data handling, recording and reporting.

The measures suggested here in terms of mitigations, protections, and alternative PNT systems will take time, effort, understanding and goodwill to implement. Until that is achieved, the maritime world can take a lead in ensuring that legacy systems and methods, including "traditional" aids to navigation and celestial navigation, are understood, taught, and used to maintain those perishable skills.

"This threat is not only to positioning and navigation; it is to every part of national infrastructure where timing is derived from space-based timing signals."

“I do not think that the wireless waves I have discovered will have any practical application.”

Heinrich Hertz – 1890

Created by the 130+ participants of the
RIN Maritime GNSS Interference Working Group.

Published by the Royal Institute of Navigation, 23rd January 2026.

Design and layout by Jemma Pentney.

Enquiries: **rpnt(at)rin.org.uk**.

Impacts of GNSS interference on Maritime Safety.
A special report by the RIN GNSS Interference Working Group.

Acknowledgements

On behalf of the Royal Institute of Navigation, I extend immense gratitude to the hundreds of people who have contributed to this report. These 120 pages are the distillation of hundreds of hours of effort from many hundreds of people.

This Working Group came together for its first meeting in September 2025 and published this report less than 4 months later. Over 130 members from across the entire industry – captains, operators, owners, authorities, manufacturers, system integrators, technical experts, industry groups, and many more – all came together, donated their time, and proposed, discussed, and debated the various findings and recommendations in this final report. For just a handful of months a lot of people gave a lot of evenings and weekends, spending time away from their families, because of their level of concern about this growing issue. To all of you that kindly gave so much time and distilled so much knowledge into these pages – thank you so much.

And finally: to everyone that currently fights the electronic fog discussed in this report to move the people and material needed to keep our economies moving and to keep the food on our table, we thank you for your hard work in the face of such adversity. Hopefully this report will play a part in easing your burden over the coming months and years.

"These 120 pages are the distillation of hundreds of hours of effort from many hundreds of people."

Dr Ramsey Faragher FRIN

Director and CEO of the Royal Institute of Navigation
Chair of the RIN Maritime GNSS Interference Working Group

Special Thanks

The main authors of this report, Ramsey Faragher and Ivana-Maria Carrioni-Burnett, would like to recognise and thank the core members of the Working Group, and in particular the following people for their contributions to various meetings, helping to write sections of this report, and for providing expertise, support enthusiasm, and the drive needed to make this activity a great success:

Bjorn Bergman (GFW), Martin Bransby (Telespazio), Stelios Christodoulou (Inmarsat), Rob Crabbe (Anschutz/ECDIS), Bridget Diakun (Lloyd's List Intelligence), Kim Fisher (IEC), Alan Grant (GLA), Kevin Gregory (IALA), Lars Grundhoefer (DLR), Warren Lester (SRT), David Pollitt RIN, Andy Proctor (RIN), Hannah Sherrard (RIN), Clare Stead (RIN), Tom Southall (IALA), Steve Vance (CGI), Lucy Woods (RIN).

Participants

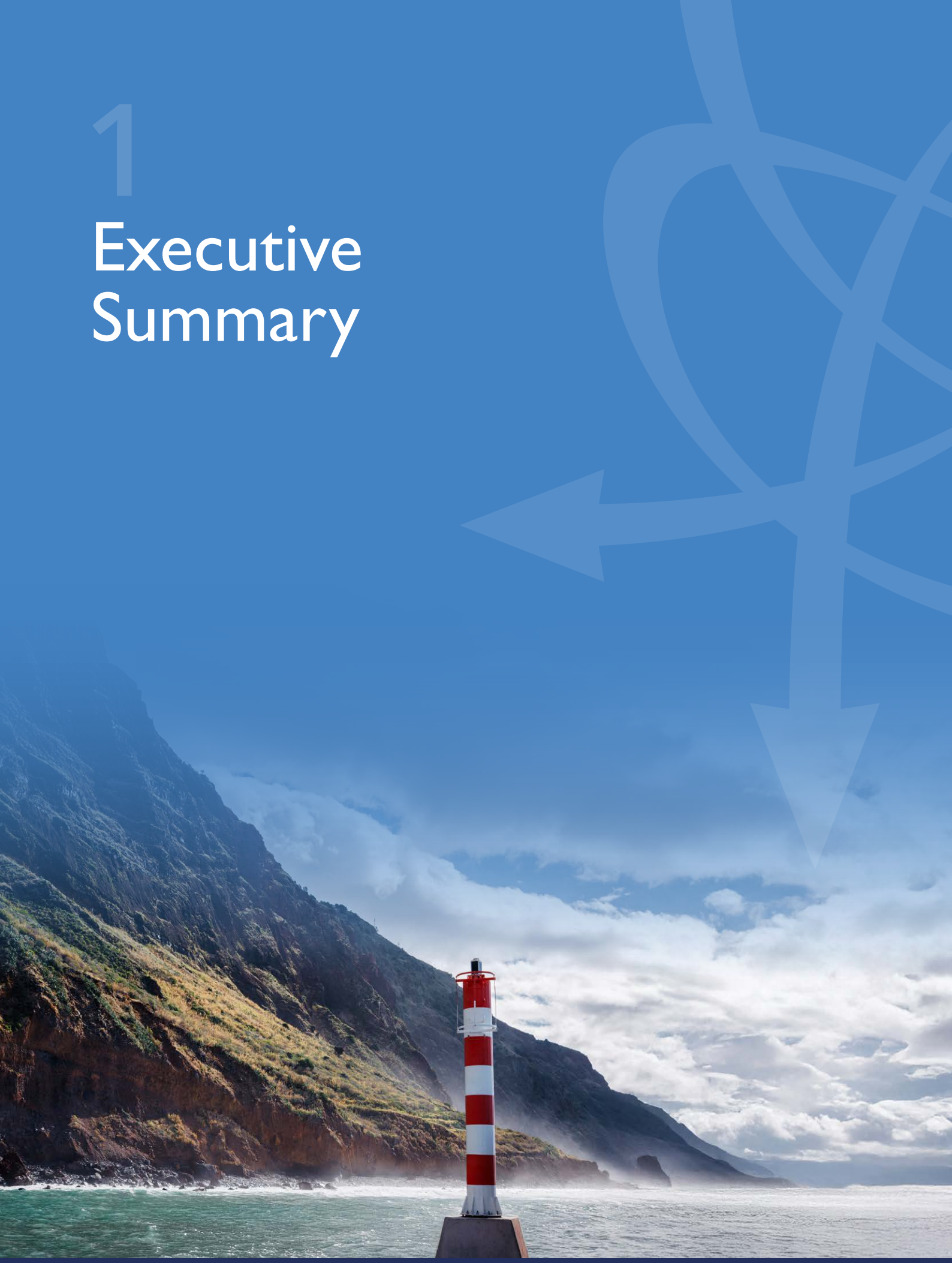
The Working Group is very grateful for the time and input of the 271 mariners who completed our survey, this data has proven to be invaluable in uncovering the scale of the problems discussed in this report.

We also extend many thanks to the 130 participants in our Discord discussion groups for their contributions and expertise, including:

Antoine Bonnet, Mikko Heikkilä, Alan Grant (GLA), Martin Bransby (Telespazio), Stelios Christodoulou (Inmarsat), Lars Grundhoefer (DLR), Rob Crabbe (Anschutz/ECDIS), Lucy Woods, Sam Sipe, Frank Williams, Dimitris Zissis, Amanda Westerman, Belen Benites, José Núñez (CUD-ENM), Rory Findlay, Eldar Rubinov (FrontierSI), Matt French, Krasimir Hristov, Goran Jedrejčić (Calian GNSS), Tom Willems (EC DEFIS), Charles Forsberg, Danny McFadden, Sam Sipe (Drogue), Emilio Pérez Marcos, Dave Martin, Nils Coe (Nortek), Hannah Sherrard, Kimon Voutsis, Kim Fisher (IEC), Jonathan Oliveira, Bart Schuitema, Warren Lester (SRT), Andy Proctor (RIN/RethinkPNT), Marco Romero, Chris Hopkins (HMCG/UKMCC), Scott Gray (Nortek UK), Stevan Harding (IMarEST), Gavin Permain, Bjorn Bergman (GFW), Marcin Dudek-Lewin, Manindra Singh, David Pollington, Okuary Osechs (ZHAW), Nitin Sharma (GNSS LabBITS Pilani), Jelle Rijnsdorp (S&T), Simon Gaskin (RIN), Maverick P (Exail), Duncan Rigg (Sonardyne), Mitch Narins, Gareth McCorkill, Steve Vance (CGI), Bridget Diakun, Kevin Heneka, Alex Haasnoot (S&T NLD), James Tidd (Swift Navigation), Ryan Kristiansen (Equinor), Paul Nevins, Jason Pool, Andrew Pickup (Hexagon), Peter van Poppel (RIN Member), Di Grazia Domenico (STMicro), Richard Turner (Hexagon), Philip Taysom (MPT & RIN), David Pollitt (RIN), Jan Šafář (GLA), Gary Kessler, Steve Thomas, Patrick Kelly (OSI), Fredy Gonzalez, Russell Pegg, Simon Booth, Clifford Slocombe, Intissar Doukali, Andriy Konovaltsev (DLR), Yemi Ogunjimi, Christoph Lass, Ahmed Telili, David Cunningham (Exail), Matthew Smith (BMT), Thomas Mellor (UKHO), Joseph Pearce (UKHO), Michael Buckley (UKHO), John Southam (Northern Standard), Rebecca Burghall (MCA), Christopher Hopkins (MCA), Richard Allen (MCA), Chris O'Flaherty (NI), and the 56 other contributors who wished to remain anonymous.

Thanks also to Kathy Hossein (RIN), Chris O'Flaherty (NI), Alan Grant (GLA), Thomas Southall (IALA), Kevin Gregory (Trinity House) and Bridget Diakun (Lloyd's List Intelligence) and all of the contributors from OCIMF for their content creation, proof-reading and feedback prior to publication.

1 Executive Summary



Intentional interference with the Global Navigation Satellite System (GNSS) radionavigation broadcasts takes many forms and is now a permanent feature of certain conflict zones and other geographical areas. In the context of this report, interference encapsulates jamming (the intentional blocking of the GNSS signals), meaconing (the recording and later rebroadcasting of real signals) and spoofing (the broadcasting of fake signals designed to force a GNSS receiver into calculating an incorrect position, velocity and time). The RIN Maritime GNSS Interference Working Group has assessed that the impact of GNSS interference on maritime safety, vessel operations, and port security is very serious, with 75% of the respondents to our survey of the opinion that this situation is not improving. This report demonstrates that the maritime industry has a widespread and deeply-integrated reliance on GNSS that needs to be carefully addressed and managed. Areas of urgent concern include:

75% of the respondents to our survey are of the opinion that this situation is not improving.

- The vulnerabilities of Global Maritime Distress and Safety Systems (GMDSS) and International Convention for the Safety of Life at Sea (SOLAS) mandated equipment that use GNSS as their primary source of position and time.
- The serious safety and liability implications associated with operating within areas of known GNSS interference using GMDSS and SOLAS equipment that are expected to fail or malfunction with high probability when in those regions.
- The evidence for unnecessary dependencies between GNSS receivers and a variety of electronic systems onboard a modern vessel, many of which do not need to be connected to GNSS data to provide their primary function. These systems include the RADAR, VHF/MF/HF radios, NAVTEX, ship's speed log, ship's clock, and satellite communications systems.

There are many well documented examples of various systems on a modern digital vessel malfunctioning during or after GNSS interference, including systems which are not primarily navigation systems. These issues are therefore impacts on end-user equipment of **cybersecurity** vulnerabilities as well as **navigation** vulnerabilities, and their assessment and management must be considered within cybersecurity frameworks. The masters of these vessels are not just dealing with the loss of access to a navigation source, they are dealing with invalid data being processed by a variety of digital systems that are vulnerable to these types of wireless attack.

The corruption of GNSS data can simultaneously compromise the Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS), RADAR, and autopilot. This can lead to a loss of situational awareness and vessel control, increasing the risk of collision or grounding, especially in congested waterways. Collisions and groundings linked to GNSS interference have included the groundings of the Meghna Princess[1] in December 2024 and the MSC Antonia[2] in May 2025, and the collision between Adalynn and Front Eagle[3] in June 2025.

[1] https://maritime-executive.com/article/union-bangladeshi-bulker-grounded-off-ust-luga-and-was-stuck-for-weeks
[2] https://supplychaindigital.com/supply-chain-risk-management/msc-antonia-risks-electronic-warfare
[3] https://windward.ai/blog/gps-jamming-falsely-placed-front-eagle-in-iran-prior-to-collision/

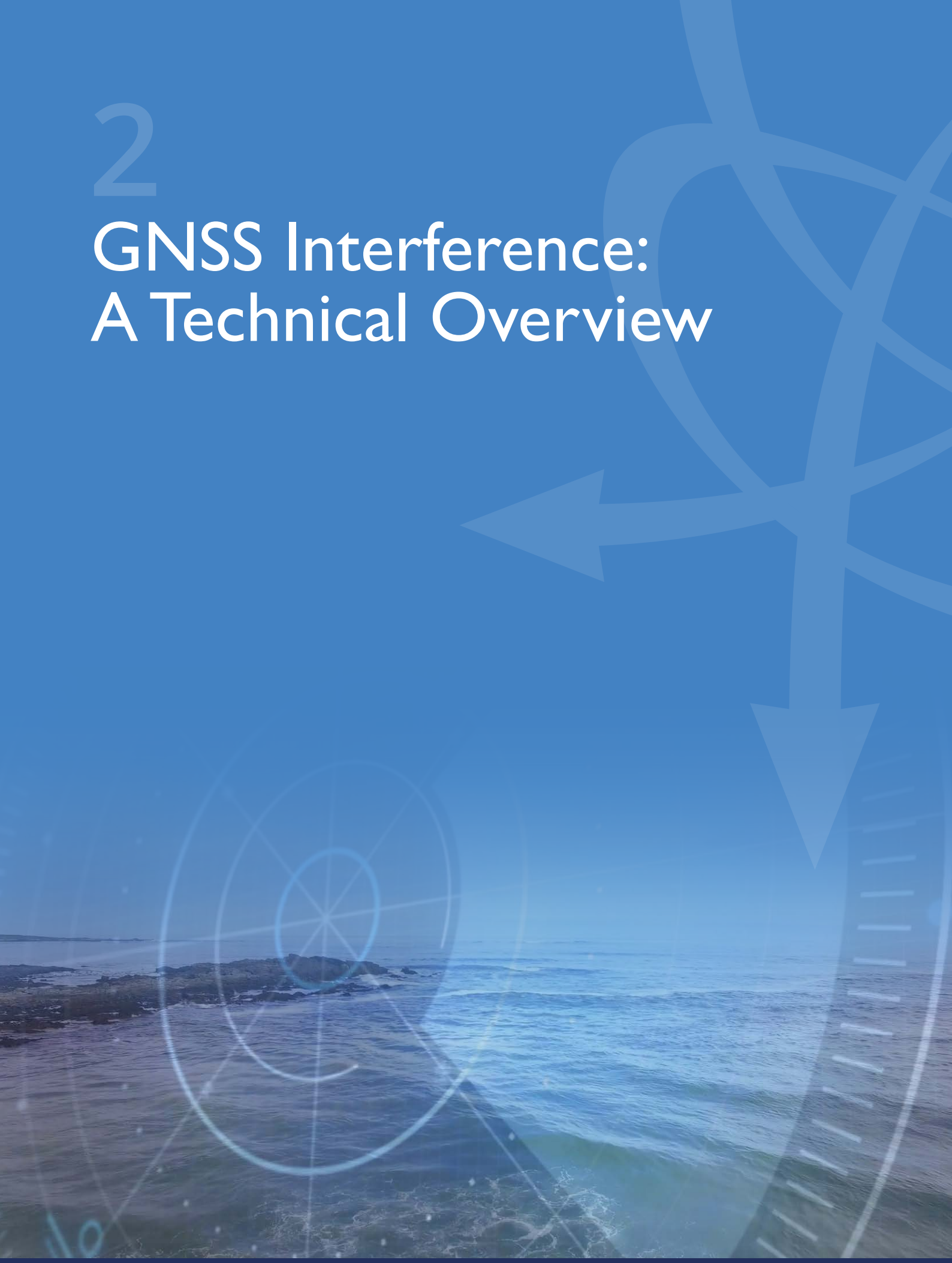
The report's recommendations include:

- Urgent addressing of the vulnerability to GNSS spoofing of SOLAS mandated systems, including GMDSS, EPIRB, AIS-SART, MOB quick-push buttons. These safety systems are mandated by the IMO but are not currently expected to operate as designed when undergoing GNSS spoofing attacks. This impacts the safety of life at sea and puts both the mariner and rescue services at risk, including delaying assistance and rescue, which has the potential to result in the loss of life or irreparable environmental damage. Equipment providers are urgently recommended to assess their products against these vulnerabilities and ensure their customers, the marine operator, is made aware of them. It is further recommended that the IMO, in collaboration with the IEC, look to provide further guidance, policy and regulation on equipment standards to address the issue of GNSS interference.
- NAVAREA Coordinators to use the World-Wide Navigational Warning Service to issue Navigational Warnings on the subject of GNSS interference in their areas. This report demonstrates the impact of GNSS interference on safety of life at sea and deems this interference to meet the criteria for "new navigational hazards and failures of important aids to navigation" as well as "significant malfunctioning of radionavigation services and shore-based MSI radio or satellite services", as determined by the Joint IMO / IHO / WMO Manual on Maritime Safety Information.
- Establishment of a real-time, global GNSS monitoring and mapping capability in order to provide timely data to the mariner, which they can use for both passage planning and situational awareness. With the advent of the new S-100 data standards from the IHO, data layers, such as a GNSS interference map, can be overlaid on an electronic chart system or ECDIS.
- Adoption of industry-wide improvements to GNSS receiver designs and their validation and testing, especially when to be used in safety critical applications. This will reduce the probability of GNSS receivers succumbing to simple spoofing attacks and will reduce the overall effectiveness of the current GNSS interference techniques in use.
- The removal of unnecessary connections to open GNSS signals by hardware manufacturers. This will reduce the number of systems that can be disrupted by processing incorrect timing or positioning data from a spoofed GNSS receiver.

Equipment providers are urgently recommended to assess their products against these vulnerabilities and ensure their customers, the marine operator, is made aware of them.

2

GNSS Interference: A Technical Overview



In normal operation, a GNSS Receiver calculates Position, Navigation, and Timing information using signals from a constellation of satellites. The publicly-accessible signals from traditional GNSS constellations are weak and are open in nature (before Galileo OSNMA was launched in July 2025[1], only military GNSS signals contained security features). In this report we use the term "GNSS interference" as an umbrella term to encapsulate all intentional disruptions, including jamming, spoofing and meaconing. Jamming is the act of overpowering a signal, either with noise or with more structured signals. Spoofing is the act of deliberately broadcasting fake GNSS signals, tailored to trick a receiver into calculating a specific position, velocity and time chosen by the bad actor. Meaconing is the act of recording real GNSS signals, and rebroadcasting them with amplification, either immediately, or at a later time and different location.

GNSS can also be disrupted by space weather and by unintentional electronic interference. These mechanisms are not considered in this report, which focuses entirely on intentional jamming and spoofing.

Intentional GNSS interference is typically carried out by a ground or air-based transmitter (or group of transmitters) and is often used in conflict zones to provide a region with some protection against drone or missile attacks. There is also some evidence that GNSS interference has been detected from space based assets[2].

Intentional GNSS interference is typically carried out by a ground or air-based transmitter (or group of transmitters) and is often used in conflict zones to provide a region with some protection against drone or missile attacks.

In principle, it is very hard to use spoofing to "capture" a GNSS receiver that is already "locked on" to the real signals. This is because the spoofing signals will appear within the receiver's processing stages ("trackers") at completely the wrong times and frequencies to be processed by the receiver. To solve this issue a spoofer would need to know the exact position, time, and velocity of the target of their attack in order to "capture" the trackers. However, an effective method of spoofing consumer GNSS receivers involves broadcasting a jamming signal first that overpowers the existing real signals coming from space. This forces the GNSS receivers to go back into "acquisition mode" where they search for satellite signals. By then broadcasting the spoofing signals louder than the jamming signal, or by alternating the jamming and spoofing, bad actors can successfully force GNSS receivers to lock onto their counterfeit signals. It seems to be an unfortunate vulnerability of many current generation receivers that their reacquisition process is very naive, allowing large jumps in position or time to occur on reacquisition, regardless of the position and time that the receiver was tracking just moments earlier.

[1] https://www.euspa.europa.eu/newsroom-events/news/introducing-new-galileo-authentication-service-osnma-join-webinar-september
[2] Z. L. Clements and T. E. Humphreys, "Transient Space-Based GNSS Interference: Observations and Analysis," presented at ION GNSS+ 2025, Baltimore, MD, Sept. 2025

Solutions to these issues are discussed in Section 6. Military receivers, and some consumer receivers with specific anti-spoofing features, provide some resistance to basic spoofing attacks. As this report highlights, future GNSS receiver designs will all need to incorporate much better anti-spoofing technologies if they are to be used in safety-critical applications. The issues of GNSS interference in the maritime sector are more serious than simply disruptions to the navigation of the vessel. On a modern digital bridge, protected by modern digital SOLAS systems, GNSS Interference can be considered to be much more of a cybersecurity problem than it is a navigation problem.

Why is GNSS Interference Happening?

The motivations behind GNSS interference in the maritime sector range from high-level state-sponsored military strategy, to avoiding international sanctions, to illicit commercial gain through illegal fishing and smuggling.

State Actors & Geopolitical Conflict

Military activities by state actors are the cause of the widespread, high-power GNSS interference that has now become a permanent feature in some waterways. In modern conflicts, Electronic Warfare (EW) such as GNSS jamming and spoofing can be used for defensive measures to protect critical infrastructure and military installations from drones and precision-guided munitions. GNSS interference may also be used to intentionally restrict freedom of movement in specific areas for extended periods of time as a result of geopolitical disputes.

The impacts of GNSS interference can be highly disruptive and dangerous, especially for commercial vessels operating nearby or within these regions. Aside from the obvious risks of collisions or groundings, there can be significant financial impacts when maritime operations are disrupted. For example, mistakes made during the installation of a cable in the Cabot strait in 2017 required a $5.9M insurance payout to replace a section of the cable that had been laid incorrectly[3]. GNSS interference could cause similar issues to this, or increase the time, cost and complexity of performing other maritime activities that build, deploy, or maintain expensive infrastructure.

[3] https://www.insurancebusinessmag.com/ca/news/construction/faulty-subsea-cable-installation-leads-to-5-9-million-insurance-payout-114101.aspx

Illicit Activities & Deceptive Shipping Practices

GNSS (and AIS) manipulations can be employed by bad actors operating on vessels to hide their own actions from authorities and commercial tracking services. Examples here include:

1. **Evading sanctions.** Vessels transporting sanctioned cargo, such as oil, can manipulate their AIS broadcasts to provide a false location, making it appear they are on a legitimate voyage while they are actually conducting a prohibited ship-to-ship transfer or port call. This could be achieved by either directly manipulating the AIS data, or else by using GNSS spoofing (AIS works by broadcasting GNSS position fixes over a radio channel).

2. **Illegal, Unreported, and Unregulated Fishing.** Fishing vessels could spoof their location to appear outside of marine protected areas or another nation's Exclusive Economic Zone while illegally harvesting resources.

3. **Smuggling, Piracy and Misdirection.** GNSS spoofing can be used to misdirect cargo ships into unsafe locations for theft or ambushes. A well-documented demonstration of this was the "hijacking" of the luxury superyacht, the White Rose of Drachs[4], by Professor Todd Humphreys in 2013.

[4] https://www.boatinternational.com/yachts/news/gps-spoofing-threat-to-superyachts-revealed-in-experiment-aboard-white-rose-of-drachs--17459

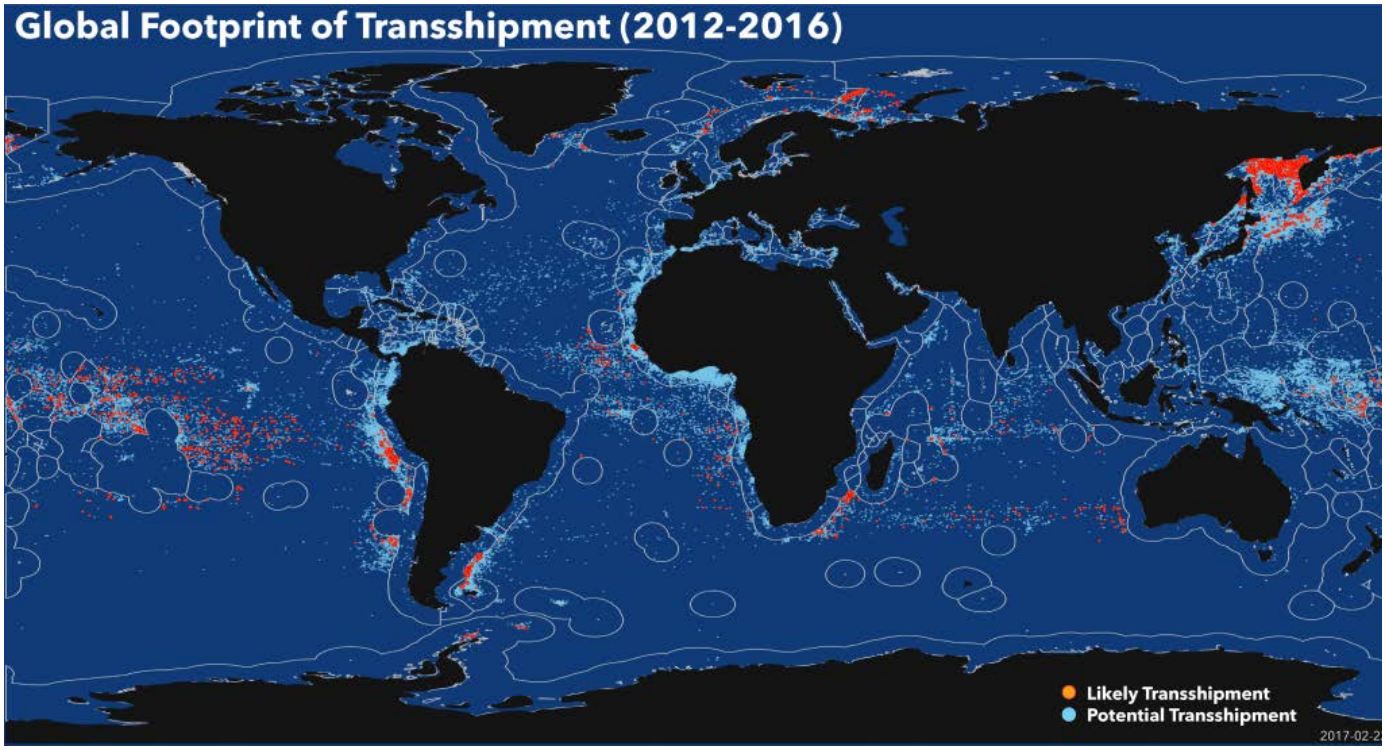


Figure 2.1 shows the estimates from Global Fishing Watch[5] of the number and location of unsanctioned ship-to-ship transfers associated with illegal fishing. From 2012 to 2016 researchers identified 5,000 likely cases of transshipment – meetings between fishing vessels and reefers. They also found an additional 86,000 cases where two reefers met at sea, which may also indicate smuggling. This map was created using AIS data; in the modern era AIS and GNSS spoofing is being used by bad actors to prevent such monitoring from taking place.

Individual bad actors

The proliferation of cheap consumer software-defined radio technology has introduced a lower tier of threat. Any suitably-motivated member of the public can source equipment, at low cost, openly on the internet that enables local and targeted spoofing of GNSS and AIS. AIS and AIS spoofing are discussed in more detail in Appendix A.

[5] https://globalfishingwatch.org/research/transshipment-report-refined/

Where is Interference Occurring?

High-powered GNSS interference affecting large areas are concentrated in areas of geopolitical tension and strategic maritime importance. The map below synthesizes incident reports and maritime advisories from 2024-2025 to illustrate the primary global hotspots. Most online maps of GNSS interference are derived from aviation ADS-B data, and so represent much larger radio horizons than are experienced by mariners. The data in Figure 2.2 below has been provided by Inmarsat[7] and is derived directly from Fleet Broadband terminals.

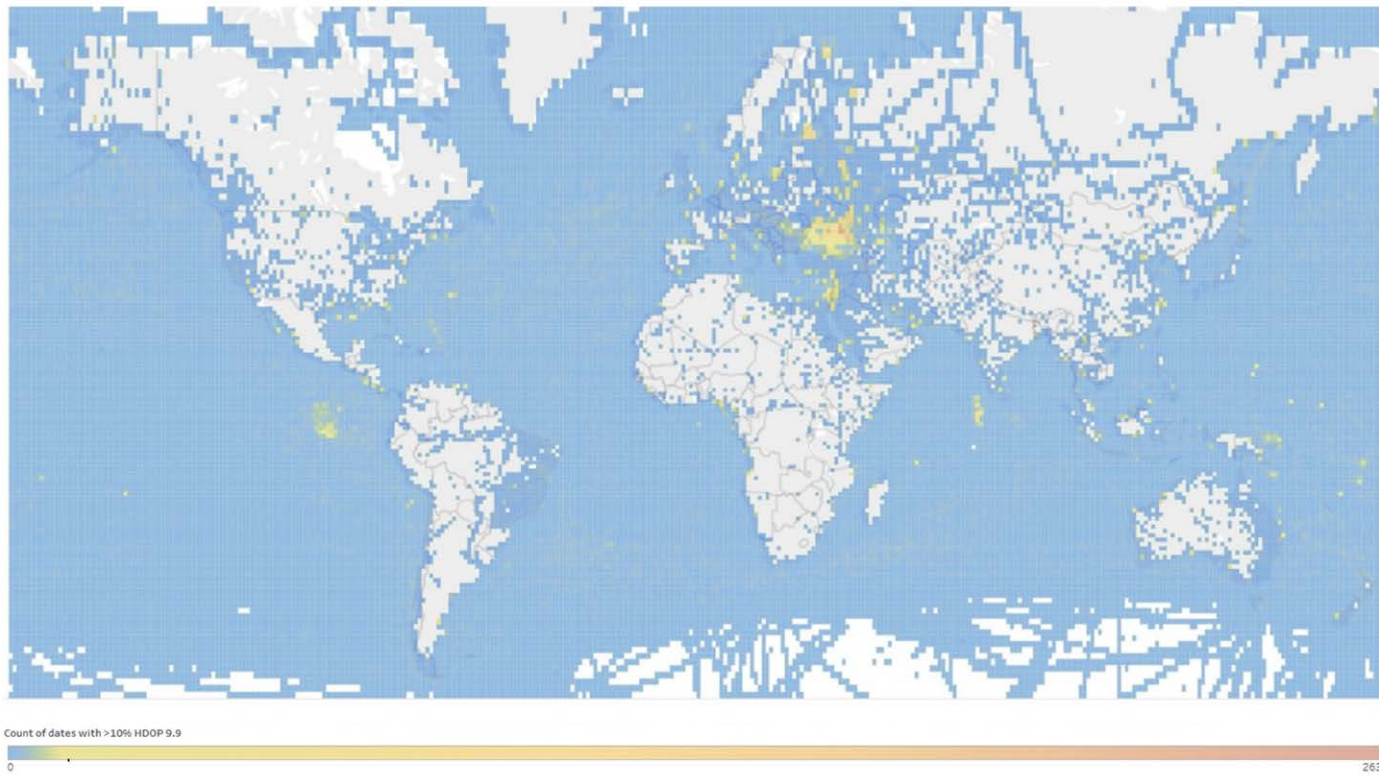


Figure 2.2 World map coloured by days of poor HDOP (representing low quality GNSS performance) in 2024 reported by Inmarsat Fleet Broadband terminals. This provides a visual representation of the global distribution and extent of GNSS interference impacting the maritime sector.

Further information on the reported interference regions from the survey is given in Section 3 of this report.

[7] https://www.inmarsat.com/

Why is GNSS so vulnerable?

GNSS interference exploits the inherent weakness of satellite signals. The satellites broadcast their messages with a transmission power of around 100Watts but these signals then travel over 20,000km to reach Earth from orbit. By the time a receiver on the Earth picks those signals up, the power level has dropped to a *quadrillionth* of a Watt (a billionth of a billionth of a Watt). This means it is very easy to overpower them with stronger nearby transmissions.

GNSS Jamming

Jamming is a brute-force "denial of service" form of electronic attack, delivered by transmitting noise (or other high-powered but "nonsense" signals) on the same frequencies used by GNSS satellites. This nuisance signal effectively drowns out the weak satellite signals, preventing a GNSS receiver from acquiring a lock and calculating a position. GNSS jamming may be accidental (e.g. from a poorly-designed piece of equipment) but there are known regions of the world where intentional GNSS jamming is now a permanent feature of that area.

By the time a receiver on the Earth picks those signals up, the power level has dropped to a quadrillionth of a Watt (a billionth of a billionth of a Watt). This means it is very easy to overpower them with stronger nearby transmissions.

Meaconing

Meaconing is a form of electronic warfare that involves the recording and rebroadcasting of navigation signals. The meaconer captures the original signal and rebroadcasts it on the same frequency, often with increased power, to create interference at the GNSS receiver. At a minimum this can result in high powered "multipath interference" which reduces the accuracy of a GNSS receiver. If the replayed data is not an instantaneous rebroadcast, then it will result in the GNSS receiver calculating the position and time of the meaconer's recording, which will be at some time in the past and may be in a completely different location. Meaconing is a significant threat because it contains valid (for that moment in time) authentication and encryption data (this is not the case for generic spoofing attacks). Meaconing is however trivially detected and ignored because the time will **always** be wrong, however for immediate record and replay meaconing this time difference may only be on the order of milliseconds. As is discussed later in this report however, it is clear that many current-generation GNSS receivers do not perform adequate checks to verify if the time being calculated by a GNSS receiver is correct or not.

Spoofing

Instead of simply jamming the signals, a spoofer transmits counterfeit satellite signals that are structured to look authentic to the receiver. The spoofer can manipulate the data within its fake signals to make the receiver calculate an incorrect but seemingly valid position, velocity, and time. The effect is a failure of data integrity, where the bridge systems continue to display a valid position and time, but one or both can be false. In the past it may have been assumed that spoofing was a technically challenging task for an adversary, however in 2026 it is trivial to source effective spoofing technology over the open internet at very low cost (e.g. $150). GNSS spoofing is both an intentional attack on navigation systems, and also an intentional cyberattack on all digital systems connected to the GNSS receiver.

Figure 2.3 A photograph taken within a GNSS interference region showing a GNSS receiver display on the bridge reporting impossible speed (SOG – speed over ground) and altitude readings.

Spoofing Patterns Observed at Sea

The analysis of AIS data, which contains GNSS fixes, provides clear visual evidence of spoofing patterns. These patterns are often signatures of specific types of spoofing attacks.

- **Circle Spoofing:** One of the most common patterns shows multiple vessels' AIS tracks moving in perfect, geometric circles. The circular pattern may be designed to bypass rudimentary anomaly detection algorithms that would flag a simple, static false position. It may also be the case that circular "example trajectories" are also the default trajectories provided by some commercial GNSS signal simulators (which may be being used by bad actors to perform their spoofing attacks).

- **Position Jumps to Land:** A frequent and obvious indicator of spoofing is when a vessel's track suddenly "jumps" from its sea lane to a fixed position on land, often an airport or a military base associated with the spoofing source. This has been widely reported in the Black Sea (jumping to Crimean airports) and the Persian Gulf (jumping to Iranian airports). Jumping to an airport is part of the drone countermeasure use of spoofing, as some consumer drones have hardcoded geofencing around airports which they will avoid approaching or will automatically land if within the zone[8]. An example of this is shown in Figure 2.4 below. This photo was taken with a Samsung smartphone, which stored the phone's GNSS position estimate in the image's exif data at the same time. The smartphone position estimate was a different inland position (54° 46.9840' N, 18° 06.8242' E) to the one being shown on the ECDIS. These positions are 22 nautical miles apart. This is a good example of how spoofing can affect different receivers in different ways, for many reasons, including different mixtures of true and spoofed satellites being used in a position fix, different constellations in use, different RAIM algorithms rejecting different satellites from the spoofed data, etc. It is important not to assume that one GNSS receiver is working and the other is not, just because they have different positions (for example one on land and one in water in roughly the correct location). It should be assumed that all GNSS receivers are under aggressive assault when in known GNSS interference regions, and their outputs should not be trusted unless known protections are in place (e.g. CRPA as discussed later in this report).

It is important not to assume that one GNSS receiver is working and the other is not, just because they have different positions.

[8] https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

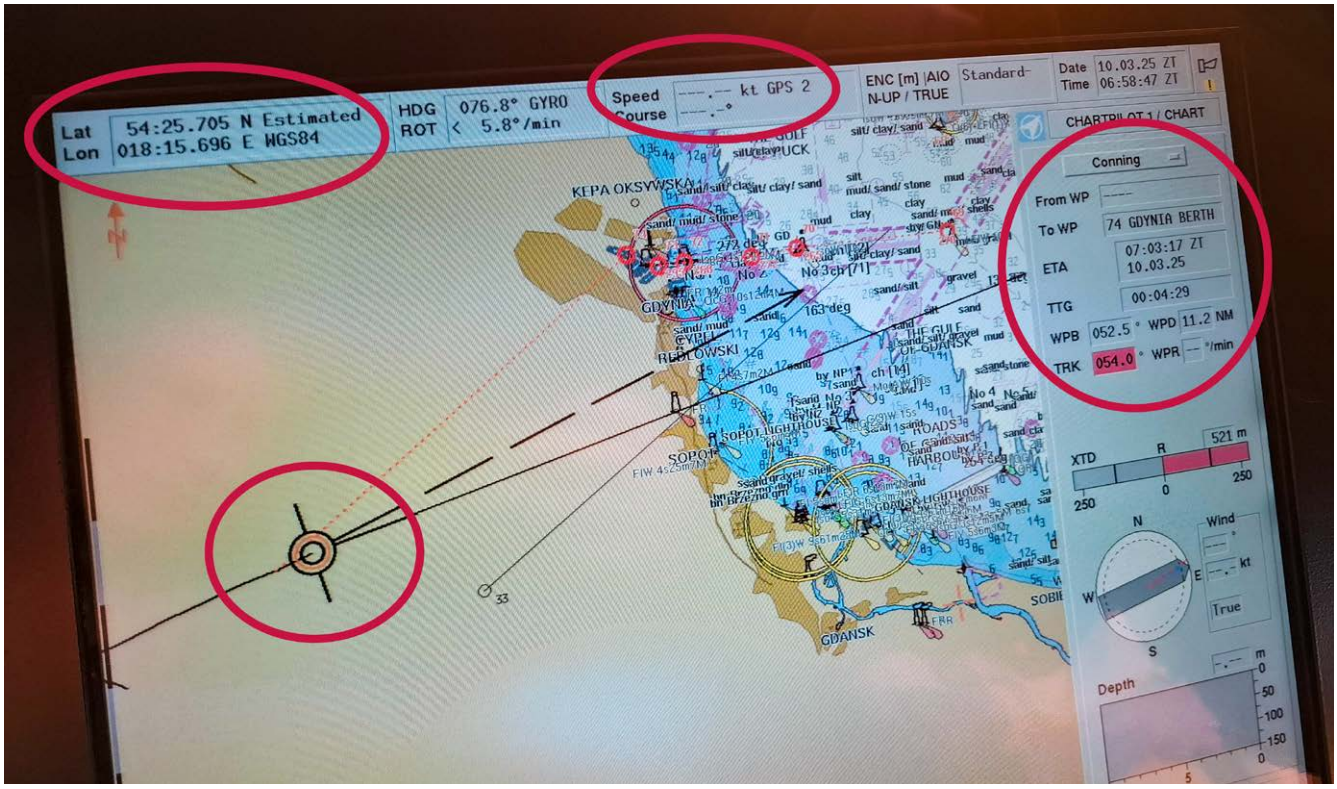


Figure 2.4 A photograph of an Electronic Chart System taken during GNSS spoofing that shows the vessel being located far inland and in motion, with a number of other data fields being absent or incorrect due to the spoofing (speed, course, Estimated Time of Arrival, etc). This vessel was in fact berthed alongside in port during this spoofing attack.

- **Sophisticated Route Mimicking:** More advanced attacks involve broadcasting a plausible but entirely false voyage track, possibly by using meaconing. This may be used by bad actors to create a digital alibi, i.e. making it appear as though a vessel is currently on a legitimate journey while it is actually conducting a sanctioned or illicit activity elsewhere. This approach may also be used to intentionally "drag" a vessel gradually off course and into foreign territorial waters or unsafe areas to cause a grounding or to "legitimately" seize a vessel.

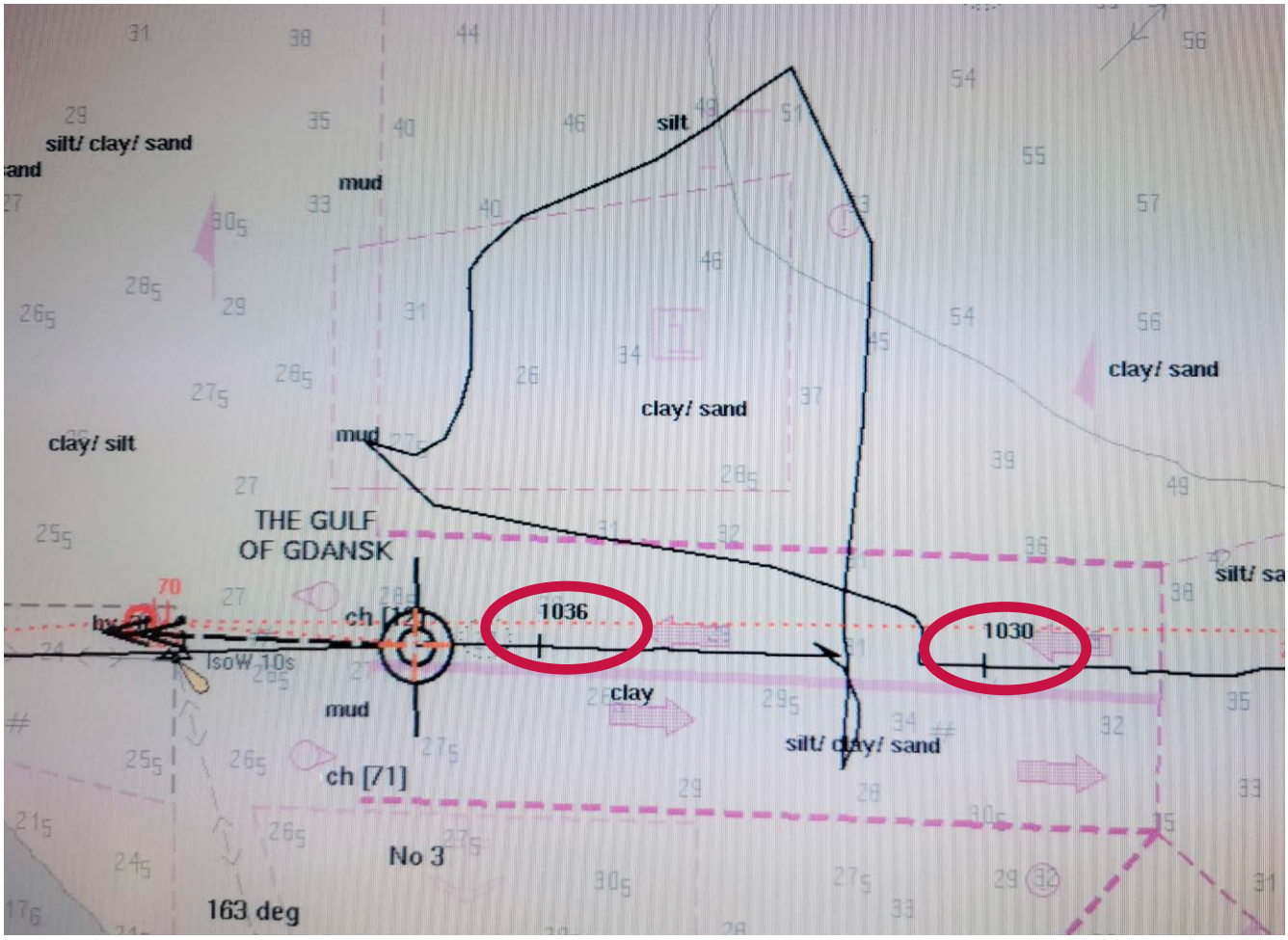


Figure 2.5 A photograph of a chart display taken during GNSS spoofing that shows the vessel travelling in an extended looping journey over several minutes that the vessel did not really take. This may have been an intentional spoofed track being broadcast by the bad actor, or it may have been the effect of the GNSS receiver struggling to process a mixture of real and spoofed signals. What is important, is that the vessel did not really traverse this complicated extended loop, it travelled directly east to west through this region.

Detecting GNSS Interference

If a bad actor is simply denying the use of GNSS to a particular region, then they will employ GNSS jamming. Jamming can be detected by a number of methods:

- The "number of satellites in use" metric displayed on GNSS receivers (on some systems this will be in a menu setting or on a secondary display) will be reading zero or a very low number, much lower than is normal for outdoor operations.
- "GNSS lost" or "GPS lost" messages or alarms may be triggered.
- Nearby vessels can be contacted using VHF radio or other means to confirm if the issue is widespread jamming or if there is a malfunction local to the vessel.
- Within the GNSS receiver, the "Automatic Gain Control" (AGC) will typically be set to its **lowest** value, but the number of satellites will remain low or zero. This is the clearest indication of jamming, as it suggests that the receiver is being "deafened" by a large input power level (and so has turned the Gain down to the lowest setting) and also cannot detect any signals. If the antenna was disconnected, or the vessel had moved under cover (e.g. under a bridge) then the AGC would move up to the **highest** setting to attempt to pick up weak signals. The AGC settings are unlikely to be available for the end user to view, but this assessment should be carried out as a basic feature of future GNSS receivers to raise a GNSS jamming alert or warning message, or should be used to provide a clear "jamming present" warning message.

Spoofing can be detected by a number of methods, but the approach depends on whether the spoofing attack is "targeted" or "generic".

In some areas GNSS spoofing or meaconing will also be in operation. In general this is employed to intentionally feed incorrect position or time information into a GNSS receiver or connected system in order to drive a particular effect. For example, this could be to attempt to crash or ground a vessel. It could also be to force incorrect time and/or date into digital systems to attempt a particular cyber attack vector (e.g. causing particular digital systems to cease operating properly). For example, this could be to try to invalidate the digital certificates on a particular system onboard a vessel, or to cause a particular system to "hang" (cease operating completely). Spoofing can be detected by a number of methods, but the approach depends on whether the spoofing attack is "targeted" or "generic", as described below.

"Generic" spoofing refers to widespread spoofing over a large area intending to interfere with as many different platforms as possible, and using the

[9] https://insidegnss.com/supercorrelation-plus-3d-mapping-aided-gnss/

same broadcast to disrupt all and any GNSS receivers within range. In these types of attacks there is no attempt at all to try to "match" the true position, velocity and time of any given GNSS receiver within range. In these instances the spoofer is exploiting the assumption that many receivers will allow large jumps in position and time if they lose lock onto satellites and are forced back into "acquisition mode".

- Detecting a "generic" spoofing attack is straightforward. The GNSS receiver undergoes a period of GNSS jamming (which itself can be detected using the approaches described above) and after a few minutes the GNSS receiver will "time out" in its attempts to continue tracking the satellites it had previously been locked onto and will revert to "acquisition mode". If the receiver then locks onto the spoofing signal, under a "generic attack" the position, velocity and time will all be incorrect. This can be determined by simply applying the laws of physics (travelling backwards in time is rather unlikely, as is teleportation, etc) or by detecting that the new position, velocity and time are in disagreement with an independent reference (a free running clock, an inertial navigation unit, a non-GNSS radio positioning system, etc).
- There is typically no attempt to ensure that a realistic GNSS received signal power is measured at the spoofed receivers. The Signal to Noise ratio may be sensible (because the spoofer is providing both the signal and the noise) and so this standard metric on its own is not useful for spoofer detection. However, as mentioned above, the Automatic Gain Control setting within the GNSS receiver may be set to a much lower value than usual for picking up real GNSS signals from the sky. Therefore if the SNR ratio is **high** but the AGC setting is **lower than normal** this is an indicator of spoofing.
- Enhanced signal processing that monitors the signal arrival angles through Doppler processing relative to an inertial measurement unit (e.g. Supercorrelation[9] can provide rapid spoofing detection and anti-spoofing capabilities against generic attacks.

"Targeted" spoofing refers to a spoofing attack that is targeting one specific vessel.

"Targeted" spoofing refers to a spoofing attack that is targeting one specific vessel. In order to attempt to overcome the basic anti-spoofing protections described above, a targeted attack may incorporate much more careful spoofing, specifically initially broadcasting the correct position, velocity and time. The target vessel's true GNSS data can be estimated using a variety of means that need not be explained here. Targeted spoofing then involves creating fake GNSS signals tailored to match these true data. Broadcasting this close match to the "true" GNSS signals allows the spoofer to attempt to "capture" the GNSS receivers on board the target vessel. This may or may not involve a period of jamming similar to "generic" spoofing. Over time the spoofer can

[9] https://insidegnss.com/supercorrelation-plus-3d-mapping-aided-gnss/

gradually vary the projected position, velocity and time in the spoofed signal broadcast to “drag” the vessel off course, or shift its estimate of the correct time. Other vulnerabilities may be exploited using the GNSS data channel.

- Detecting a “targeted” spoofing attack involves more careful assessments than for a generic attack. It is still the case that the power level may be higher than for the true signals, so a test involving the SNR and the AGC should still be employed.
- Careful comparisons of position, velocity and time against completely independent references are required to detect and alarm against targeted spoofing. A highly stable clock disciplined to UTC using non GNSS sources, access to a high quality inertial navigation system, and access to alternative radio-navigation aids are highly recommended for detecting a targeted spoofing attack.
- Galileo OSNMA is discussed in Section 6 and provides a mechanism for detecting targeted spoofing has occurred.
- Controlled Reception Pattern Antennas that use beam steering and monitor the angle of arrival of GNSS signals provide an important defence against all jamming and spoofing, including targeted attacks.

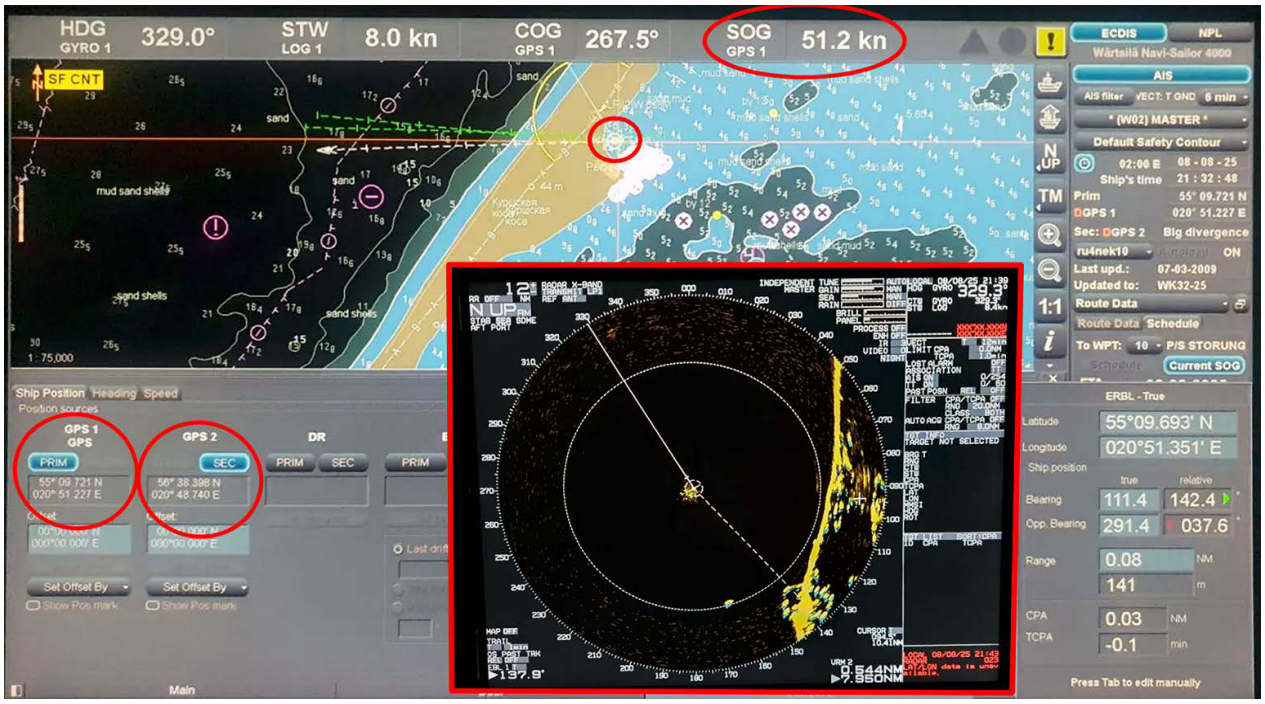


Figure 2.5 A photo of an ECDIS displaying the vessel moving at an impossible speed towards / over a spit of land and the corresponding RADAR image (inset image). The ECDIS is showing both GPS inputs, which do not correlate with one another, and the RADAR shows no position input. The heading and speed through the water (STW) on the ECDIS correlate with the RADAR image so we can determine that the vessel is in fact to the west of the land shown, at a range of approximately 8nm, proceeding in a north-westerly direction, at a moderate to slow speed and NOT heading west, towards land, at speed.

Monitoring GNSS Interference

The effectiveness of all mitigation and resilience measures described in this report depends on the ability to detect, characterise, and understand GNSS interference in operational environments. GNSS interference monitoring does not, in itself, prevent or defeat jamming or spoofing, although it can provide advanced warning during route planning to avoid exposure to known GNSS interference regions. Interference monitoring provides the foundational evidence required to inform when and where specific solutions are justified, how they should be configured, and how their performance should be assessed.

At an operational level, monitoring supports situational awareness and decision-making in GNSS-degraded environments. When aggregated and assured at fleet, national, or international level, monitoring data enables the identification of persistent interference patterns, supports regulatory and standards development, informs investment decisions in resilient PNT, and contributes to post-incident analysis and accountability. GNSS interference monitoring should be regarded as an enabling capability that underpins the selection and application of the various solutions and mitigations available.

GNSS monitoring is also vital for understanding the bigger picture regarding the particular constellations and frequencies being attacked in a given region. A common assumption is that multi-frequency and multi-constellation receivers may provide some protection against jamming or spoofing, but the success of such a strategy in 2026 is based more on luck than technological advantage. Multi-band, all-constellation jammers and spoofers are widely available.

Figure 2.6 A screenshot from CGI SignalSence showing observed GNSS interference on multiple frequencies at selected maritime choke points from August 2024 to February 2025. Source: Aggregated GNSS interference monitoring data by a commercial monitoring service (CGI SignalSense).

3 Survey Results

The survey accompanying this report was open for the autumn and winter of 2025, and all of the data given here is the compilation as of 1 December 2025. The survey will remain open to continue gathering data beyond the publication of this report, to allow for future longitudinal analyses. As of 10 January 2026 there were 271 respondents, and the distribution of these respondents by role is given below. Given the public nature of the survey, the inability to perform any control measures, and the "good faith" basis for the honesty of the answers being provided, it is expected that there is inevitably some margin of error on the quantitative results. The sheer number of respondents gives some confidence however in the overall qualitative findings that can be drawn, such as whether opinions are strong or weak on a given matter, and categories that have high and low proportions. Given the above we propose using the standard formula for the frequentist Margin of Error[10] which leads to a standard error of ±6% for data with a sample size of 271. Therefore all quoted results should be assumed to have this error associated with them, and any statistic lower than 6% should also be considered to be too unreliable to draw a firm conclusion. Some questions were not answered by all respondents, and where relevant this is discussed in the appropriate subsection.

The sheer number of respondents gives some confidence however in the overall qualitative findings that can be drawn, such as whether opinions are strong or weak on a given matter.

Respondents

The distribution of respondents by vessel class was **61% tankers, 14% container/cargo, 4% passenger/ cruise ship, 4% offshore installation and the final 17% were drawn from a very large set of categories** (e.g. tugboats, private yachts, military vessels, maritime search and rescue craft).

The job roles of the respondents were distributed as follows: **57% were Captain/Master, 24% were Chief Mate/Officer of the Watch/Cadet, 9% were a superintendent, and the remaining 10% were drawn from a large set of categories** (e.g. owner, client, dock master, VTS officer, DP officer, inspector, trainer).

The survey consisted of 31 questions, and the aim was to determine the impacts being experienced on maritime platforms during and after encountering GNSS interference. This section explores the findings of the survey in detail. An anonymised subset of the survey results are available to researchers and other interested parties (contact the Royal Institute of Navigation for access).

[10] Wonnacott, T.H.; R.J. Wonnacott (1990). Introductory Statistics (5th ed.). Wiley. ISBN 0-471-61518-8.

Confidence in systems

When asked about the confidence that the respondents had in using their systems to detect GNSS jamming and spoofing, 20% of the respondents were not confident that their systems could easily detect **GNSS jamming**, and 27% of the respondents were not confident that their systems could easily detect **GNSS spoofing** (see Figures 1 and 2). The distribution was similar for **AIS spoofing**, with 36% of respondents expressing low confidence in the use of their systems to detect AIS spoofing.

Do you **agree** or **disagree** with this statement:

I am confident that the systems I operate make it **easy for me to detect jamming** (the blocking of GNSS signals)

271 responses

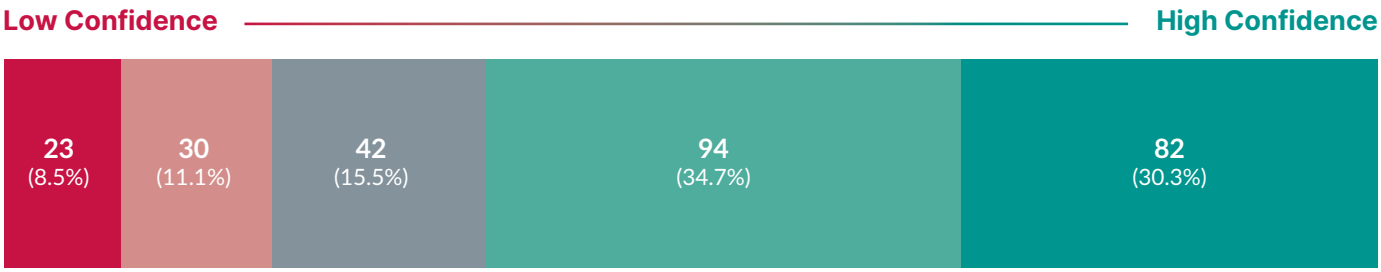


Figure 3.1 - Respondents level of confidence in detecting GNSS jamming

Do you **agree** or **disagree** with this statement:

I am confident that the systems I operate make it **easy for me to detect GNSS spoofing** (the broadcasting of fake GNSS signals to make a GNSS receiver calculate an incorrect position and/or time)

270 responses

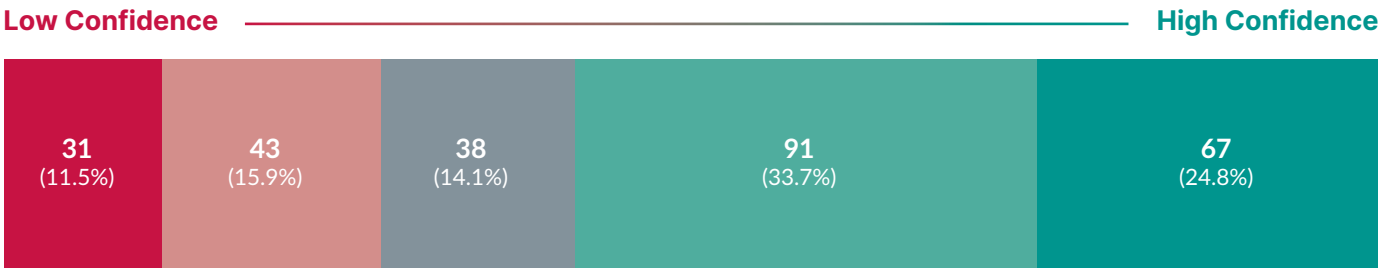


Figure 3.2 - Respondents level of confidence in detecting GNSS spoofing

Do you **agree** or **disagree** with this statement:

I am confident that the systems I operate make it **easy for me to detect AIS spoofing** (intentional misleading AIS broadcasts)

269 responses

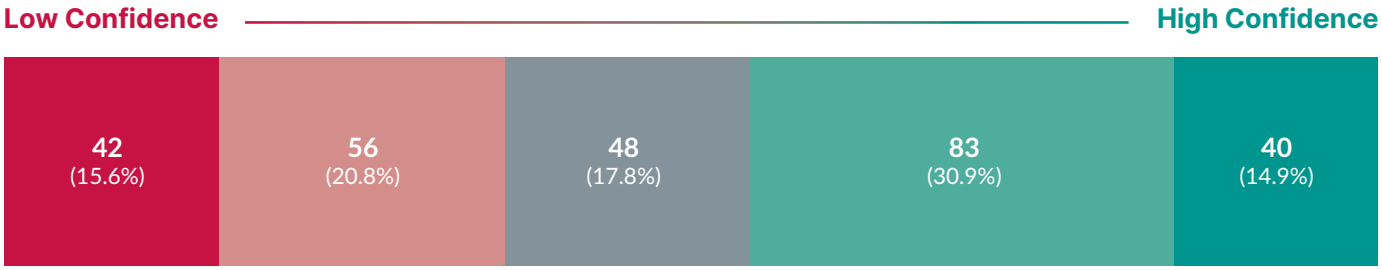


Figure 3.3 – Respondents level of confidence in detecting AIS spoofing

Experiences with GNSS interference

Of the 271 respondents, 212 reported that they had experienced GNSS interference (79% of those surveyed).

The questionnaire explored where respondents have experienced GNSS interference globally. The data (Figure 3.4) from the questionnaire agrees broadly with independent information from public GNSS interference maps (eg https://gpsjam.org/), with more interference having been experienced in the Baltics, Black Sea, Caribbean Sea, Mediterranean Sea, Red Sea, Persian Gulf. Some interference has been experienced in the South China sea, but very little has been experienced in UK and USA coastal waters. Around 2% of the respondents reported that the UK and USA regions had experienced GNSS or AIS interference, but this proportion is lower than the margin of error (±6%) for the size of this dataset, and so no firm conclusion can be drawn here (i.e. those responses were so rare relative to the sample size that they could have been caused by accidental/erroneous survey selections). By comparison in the Persian Gulf, over 80% of those who had been in that region had experienced GNSS or AIS interference.

Figure 3.5 demonstrates that even within the most interfered regions, there are still a noticeable number of reports of “no impact” by some respondents. This is likely to be either due to some vessels already having suitably robust equipment onboard capable of defeating the interferences, or is evidence that interference is not covering 100% of these entire regions, or is not enabled 100% of the time. For example, roughly ⅓ of respondents reported daily interference in the Baltics and roughly ⅓ of respondents stated no interference at all in the Baltics. This difference is likely to be caused by

different respondents moving through different regions within the Baltics (interference is shown to be more common in the Eastern region of the Baltics than the Western region of the Baltics).

Have you or your crew **experienced GNSS interference** (jamming or spoofing) in any of the following **regions**? (Please put at least one tick in each row.)

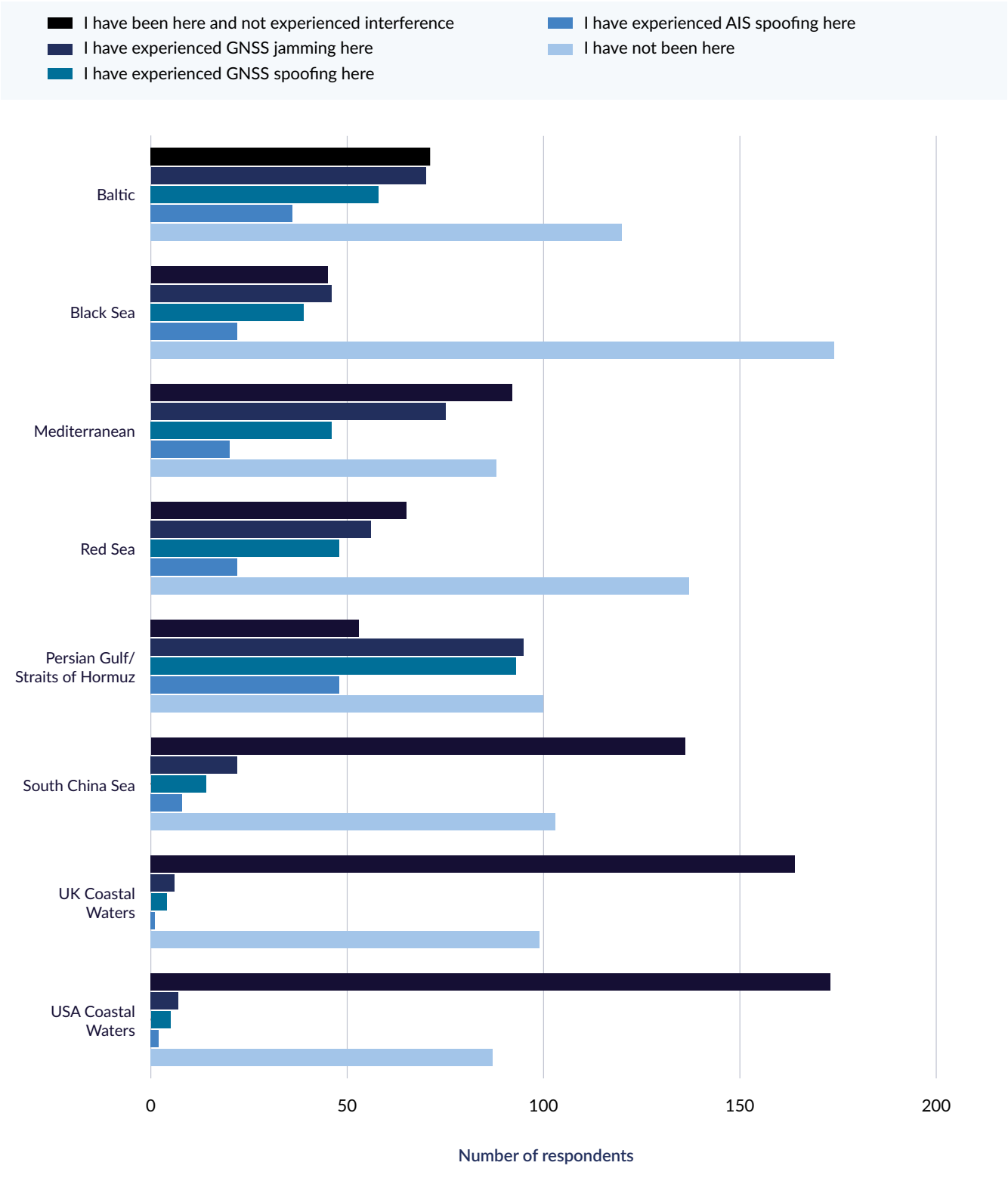


Figure 3.4 shows the distribution of reported interference events by region.

Expanding on the adobe question, for the regions where you have encountered GNSS interference, please give an estimate of **how common GNSS interference is in the region**. (You can leave rows blank in this question.)

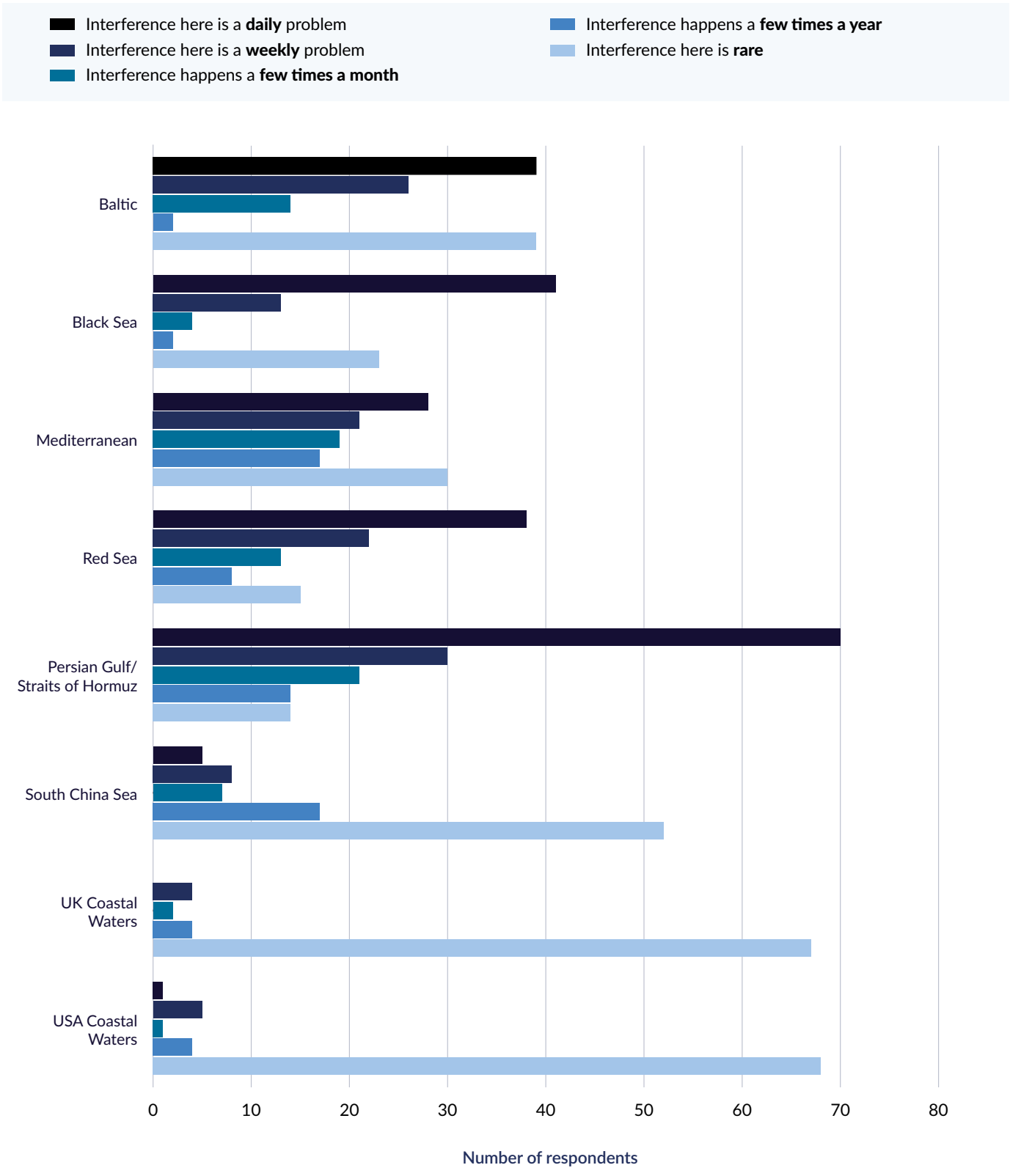
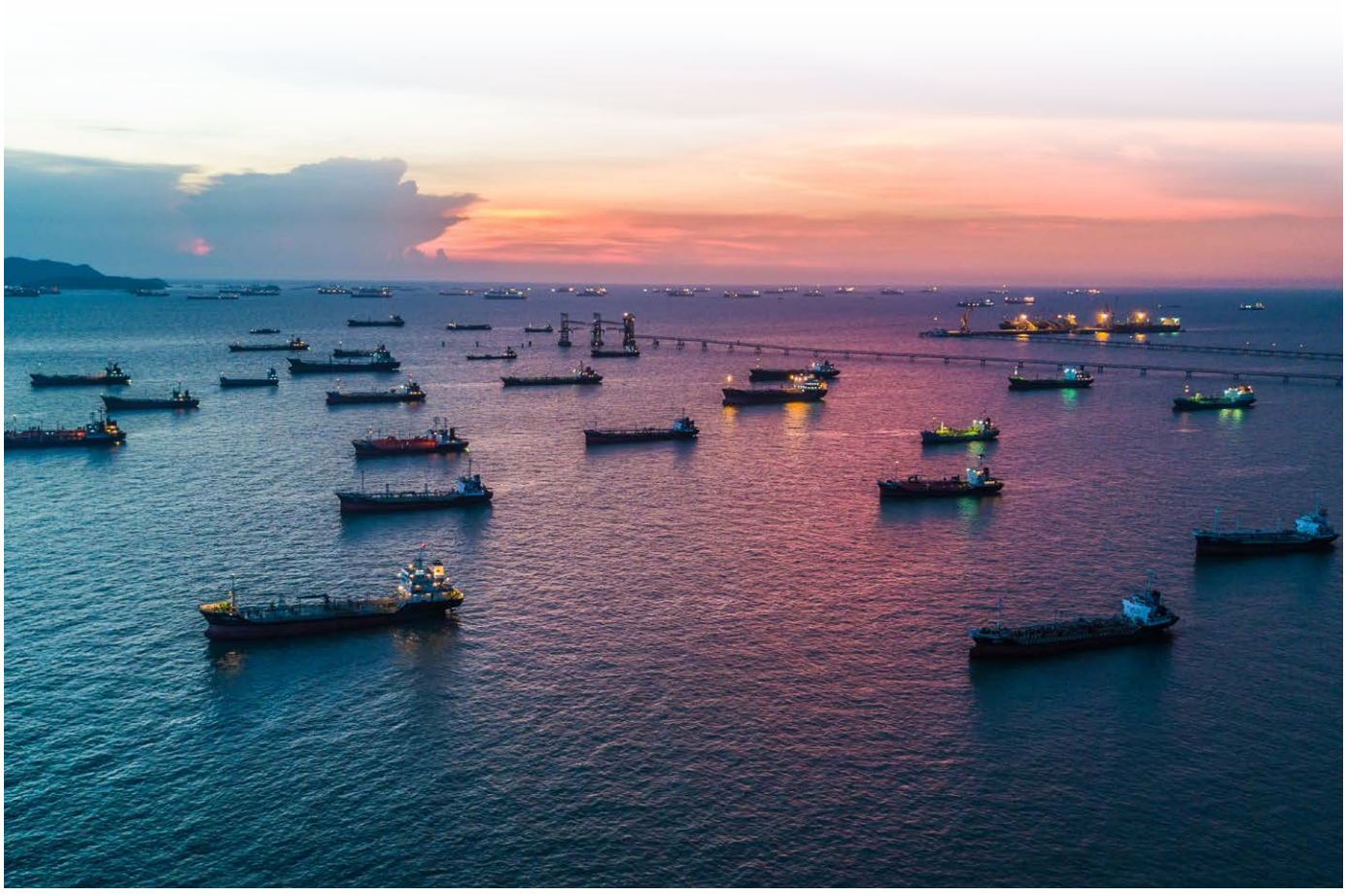


Figure 3.5 shows the reported prevalence of interference by geographical region.

The respondents were asked how long they notice the effects of interference on their systems in each of these regions, and the results are shown in Figure 3.6. In the regions where GNSS interference was most common, disruptions lasting for a day or longer have been reported. In the worst affected region (the Persian Gulf) it was reported that more than 50% of the time that interference is encountered, it impacted the vessel for many hours or more than a day.



Expanding on the above question, for each region where interference has been experienced please select **how long your experience of incorrect GNSS data being displayed lasted** (select as many as apply, e.g. if you have experienced just a few minutes of problems one day, and many hours another, in the same region, then please select as many boxes as apply)

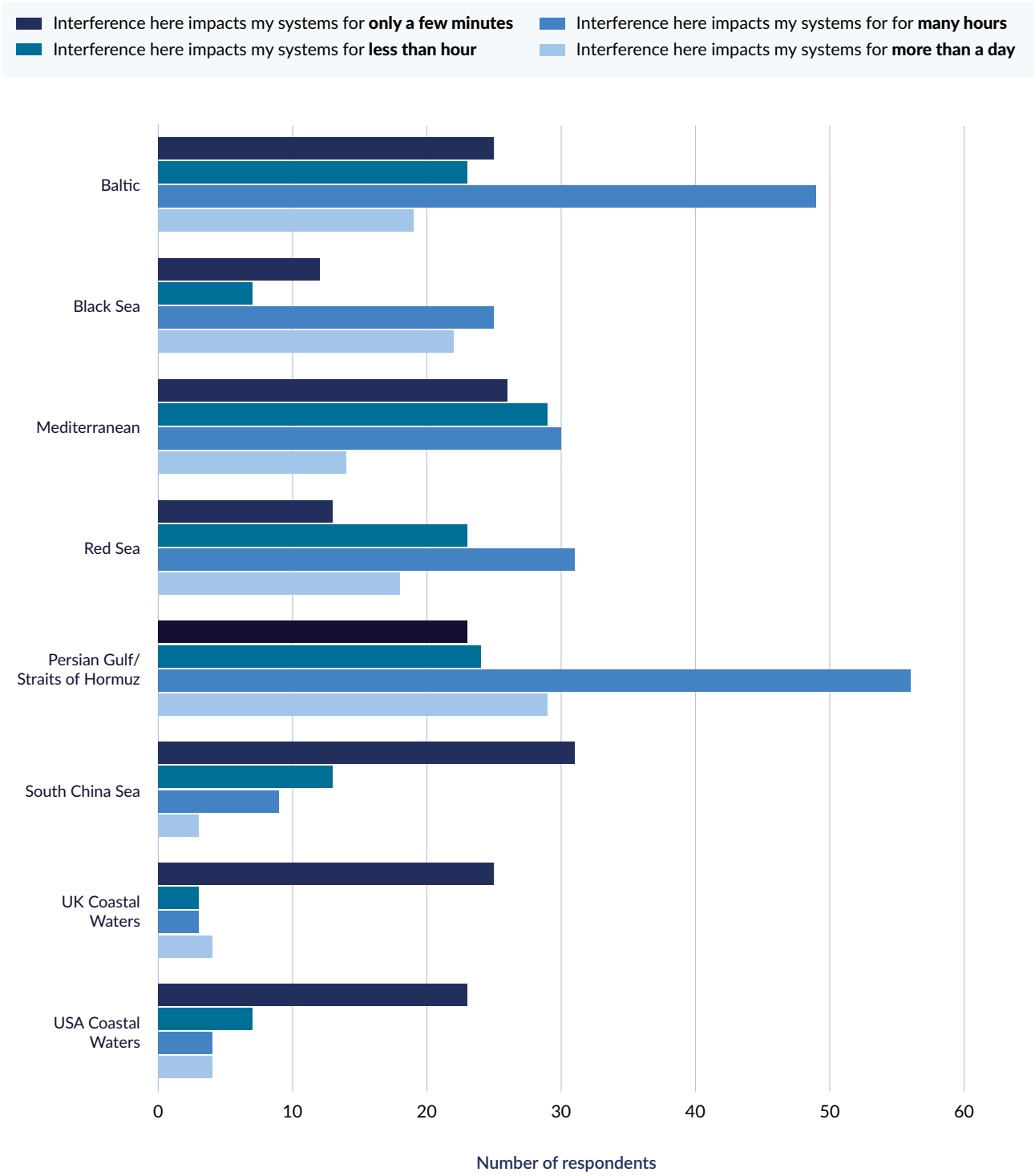


Figure 3.6 shows the reported impact of GNSS interference on vessels in various regions in terms of how long systems are affected by the interference. The options for selection were whether the impact on the vessel's systems were just a few minutes (blue), less than an hour (red), many hours (yellow), more than 1 day (green).

A clear statistic derived from the survey is that 75% of respondents believe that the problem of GNSS interference is remaining consistent or getting worse. Only 3% of respondents reported that they believe that the problem is getting better for them specifically because they have installed new hardware to counter the problems (although this result is so rare that it is within the statistical margin of error[11]).

Figure 3.7 below provides the data on the number of systems that have been reported to be affected within regions of GNSS interference. The systems reported to be impacted the most often include the GNSS receiver (85% of respondents), AIS (75% of respondents), ECDIS (70% of respondents) and RADAR (51% of respondents). This proportion of people reporting issues with their RADAR is of particular concern, as the use of RADAR systems combined with a Doppler log should be capable of operating entirely independently of GNSS for collision avoidance when set-up correctly for this purpose, as well as ranging for navigational purposes. It is possible that these issues are related to modern RADAR software using GNSS inputs such as position, speed and heading for various display features. For GNSS receivers, AIS, ECDIS and RADAR, the survey results suggest that around 5% of the respondents have seen residual issues with the systems long after leaving the GNSS interference regions, and around 10% of the respondents reported specific errors in the display of time and/or date on those systems.

Systems that historically have not required any access to GNSS data in order to function, such as the VHF,MF/HF and NAVTEX radio systems are also reported in the survey as being disrupted during GNSS interference, with 29% of respondents reporting issues with their VHF,MF/HF radios, and 15% reporting issues with NAVTEX.

Issues with satellite communications were reported during GNSS interference by 33% of respondents. Satellite communications systems are likely to use GNSS position and time information in order to search in the correct direction in the sky, and in the correct frequency range, to acquire and track the satellites orbiting overhead.

Of most concern are the SOLAS (Safety of Life at Sea) required equipment and systems, with 7% of respondents reporting that they had **seen the time displaying incorrectly on SOLAS required systems during GNSS disruption**. This is a strong indicator that the GNSS receiver integrated into this system was undergoing a spoofing attack at that moment, and if a GNSS receiver is calculating the wrong time it is highly likely that it is also calculating the

[11] A larger sample size is needed to confirm this statistic, as such a small number of tallys of this option could also have been caused by a few respondents accidentally ticking the wrong box when completing the survey

wrong position. The concern here is that in each of these cases, had an emergency had occurred at that instant the associated SOLAS equipment would have transmitted incorrect location data as part of its distress message.

Similarly 35**% of the respondents reported GMDSS being impacted during GNSS disruption**, with **11% of respondents specifically reporting time being displayed incorrectly on their GMDSS**. Again, this suggests that there is clear evidence that these emergency systems can report incorrect information in their emergency broadcasts during these instances. This includes the quick-push DSC (digital selective calling) function on the GMDSS communications equipment and quick-push MOB (man-over-board) functions which are supposed to be available for immediate use in the case of an emergency.

20% of the respondents reported GMDSS being impacted during GNSS disruption, with 11% of respondents specifically reporting time being displayed incorrectly on their GMDSS.

The most important recommendation of this report is that these issues are investigated and addressed urgently by the maritime community.

The other systems that the survey respondents indicated were known to be impacted during GNSS interference were: gyrocompass, autopilot, Doppler log, ship's clock, VDR, DP, SSAS (Ship Security Alert System), VMS, and INS.

On your vessel or platform, **which items listed are being impacted by GNSS interference** when it occurs, either directly or indirectly? Does the item only exhibit problems during the GNSS interference, or does it also remain faulty/problematic long after the GNSS interference has ended? **Specifically, have you noticed this item's display of the time/date being incorrect during or after GNSS interference?**

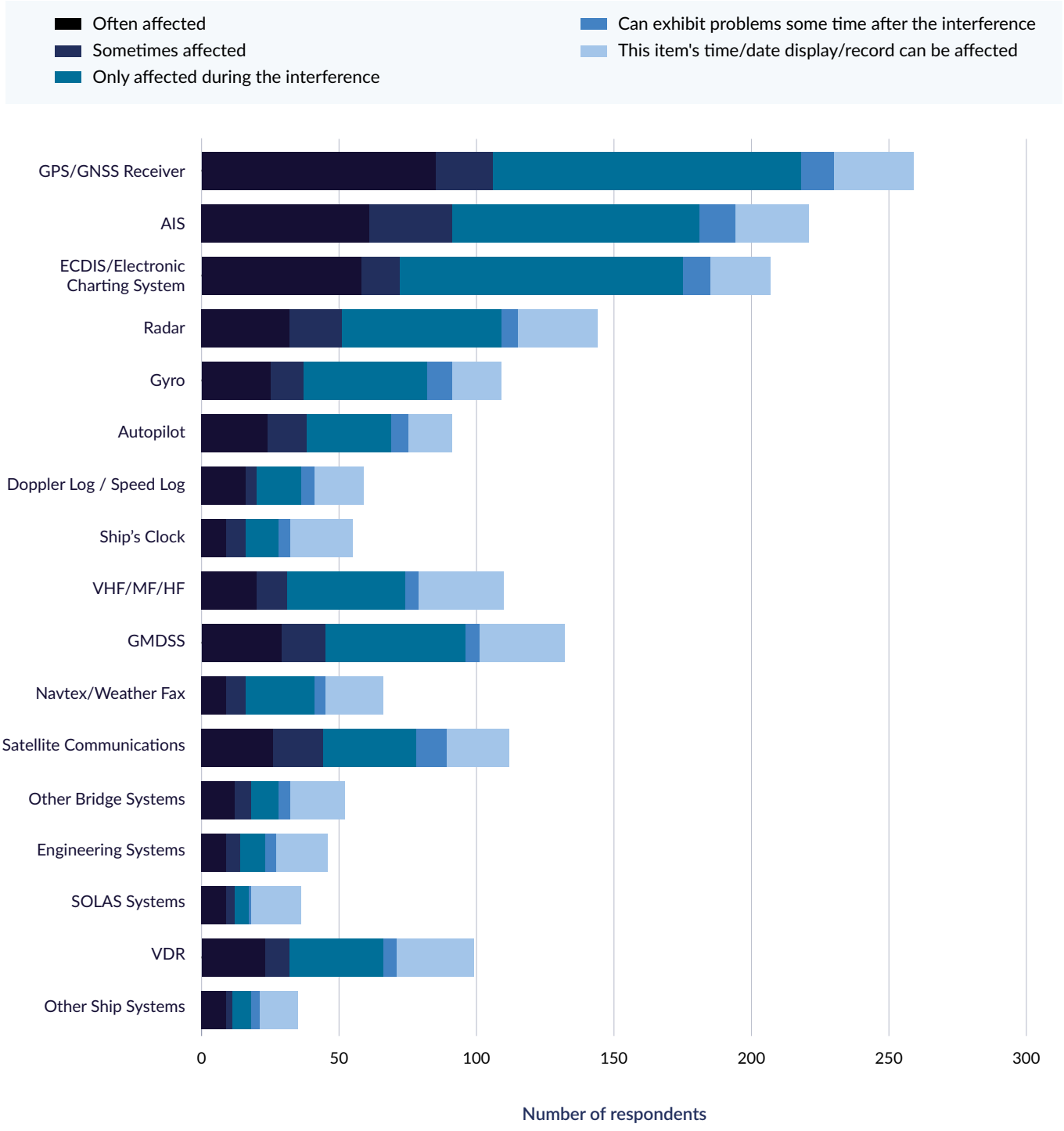
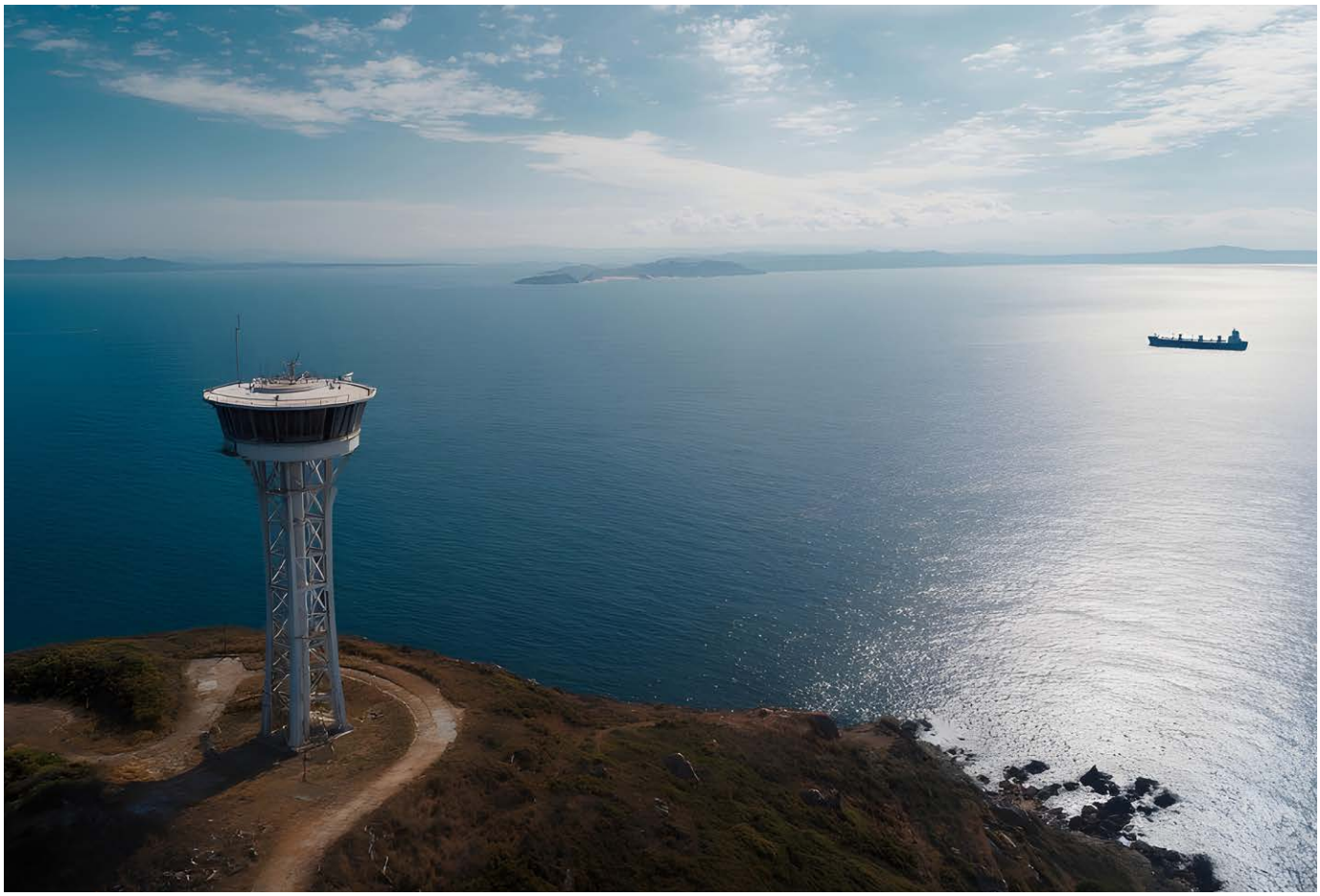


Figure 3.7 shows the digital systems onboard modern vessels that are reported to be impacted by GNSS interference.

Effects and attempted mitigations

The survey asked the respondents how well their systems had recovered after interference, and specifically whether they had been damaged or needed manual interventions. The degree to which the different systems appear to recover on their own or need manual interventions seems to be variable, which is to be expected given the wide variety of manufacturers and models of maritime digital systems.

For GNSS receivers, it was reported that the system needed to be manually adjusted or power cycled 20% of the time in order to recover fully from interference. There were no reports of the device being permanently damaged and having to be completely replaced. The other systems that were reported to need power cycling or manual interventions to ensure recovery from interference regions were the AIS, ECDIS, RADAR, gyro, autopilot, ship's clock, VHF,MF/HF radios, GMDSS and satellite communications. For these systems, the reported proportion of times that they required manual intervention was in the 10-20% range. A more detailed breakdown is shown in the figure below.



Where relevant, **how well have these systems recovered after interference.** Have they ever been damaged?

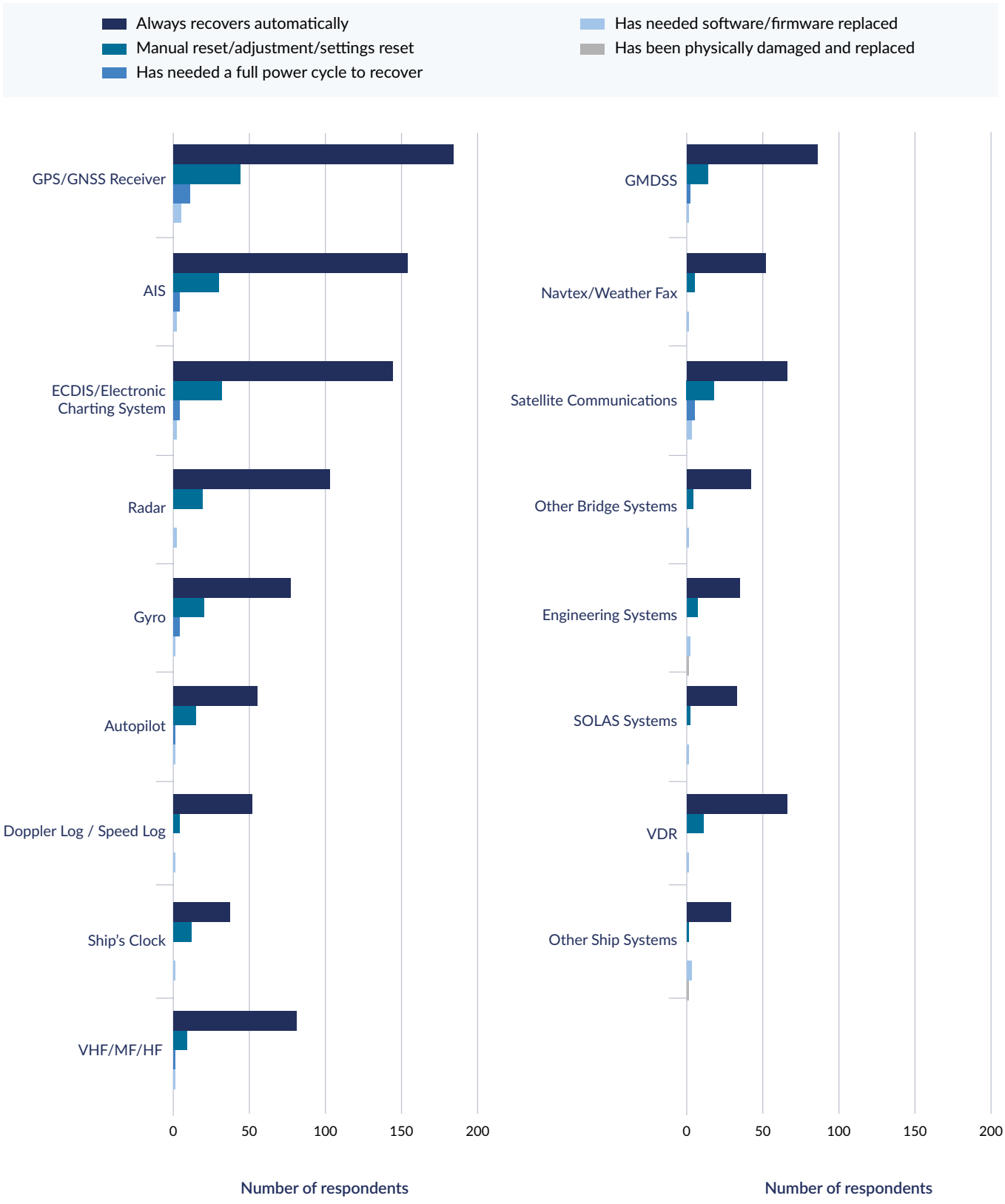


Figure 3.8 shows the distribution of recovery successes after encountering GNSS interference for each of the systems surveyed.

The survey asked how the respondents had confirmed that their systems had returned to normal after interference. The most common reported method was a RADAR position fix (87% of respondents). This is of concern, given the information from earlier in the survey suggesting that the bridge software displaying RADAR data can alarm and require interventions during GNSS interference around 50% of the time, typically due to the loss of GNSS data preventing various display features from being available. It is expected that the core RADAR transmission and receive functionality are not affected directly.

The second most common way to confirm that the GNSS receiver had recovered after interference was by using an alternative GNSS fix. This was cited to be applied 56% of the time. **This is particularly risky, and is not recommended**, unless there are clear reasons to expect that the alternative receiver will have anti jamming or anti spoofing capabilities (e.g. it is fitted with a CRPA). When in a region of intentional and aggressive GNSS interference it should be assumed that all "simple" GNSS receivers are low in integrity and are just as likely to be reporting incorrect information as the "primary" affected receiver. It should also be assumed that the GNSS interference may evolve over time and as the vessel moves through a region, such that different GNSS receivers may fail in different ways at different times. Around 26% of respondents reported verifying that the affected GNSS receiver's time display matched an independent source (e.g. wristwatch) as a method of determining when the GNSS interference had ended. Celestial navigation was reported to be used 27% of the time, and taking a horizontal sextant angle was reported to be used 10% of the time, to determine that GNSS interference had ceased. It is also important to note that some smartwatches contain a GNSS chipset, and a smartwatch can also be spoofed. Take this into account before using a wristwatch as a reference for the "correct time" in a GNSS interference region.

"26% of respondents reported verifying that the affected GNSS receiver's time display matched an independent source (e.g. wristwatch) as a method of determining when the GNSS interference had ended."

How did you **confirm that your systems has returned to normal** after interference? (Please tick all that apply, or give further information at the end of the list.)

239 responses

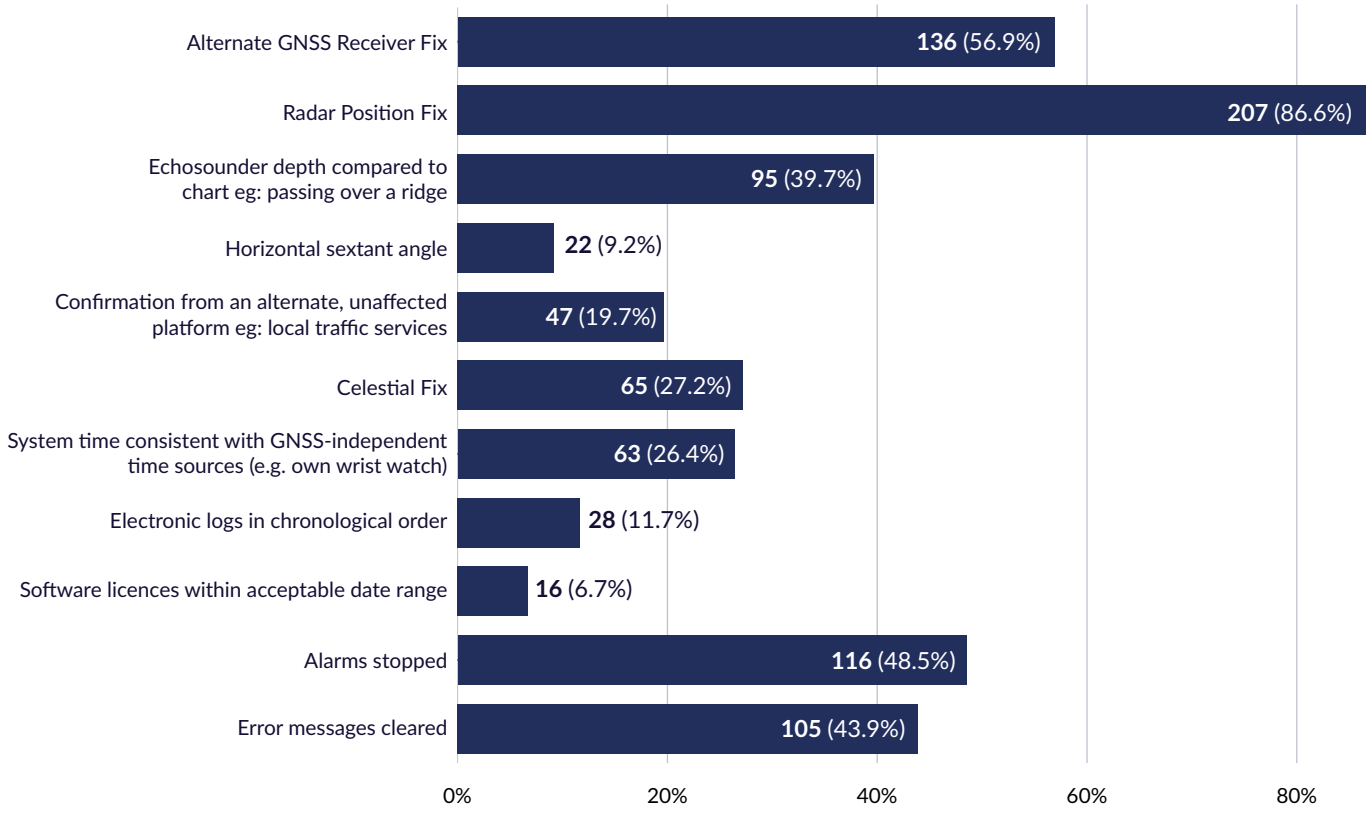


Figure 3.9 shows the methods employed to assess that GNSS interference had ended.

In terms of navigation actions taken during the GNSS interference itself, 88% reported using dead reckoning, 45% reported selecting an alternative GNSS receiver (note the warning against this cited in the previous paragraph) and 8% reported no action other than to silence the alarms.

Only 71% of respondents reported the interference after encountering it. Almost 40% of respondents reported that they either informed their system provider, requested a resolution from them, or paid for a new system. 4% stated that they changed their route.

Around 75% of respondents reported that the interference regions have a moderate or large impact on their workload.

Increases in workload were countered by adding more personnel to the bridge (61%) and reducing speed (30%). In 19% of cases the respondents reported either changing route, stopping all operations, or proceeding to anchor.

Figure 3.10 shows the impact that the GNSS interference has on vessel safety, personal safety/wellbeing, crew or passenger safety/comfort and cargo control. **There are clearly serious concerns with regards to safety of the vessel (67%) and personal safety/wellbeing (56%). There are lower but still noteworthy concerns with crew/passenger safety (50%) and cargo control (30%).**

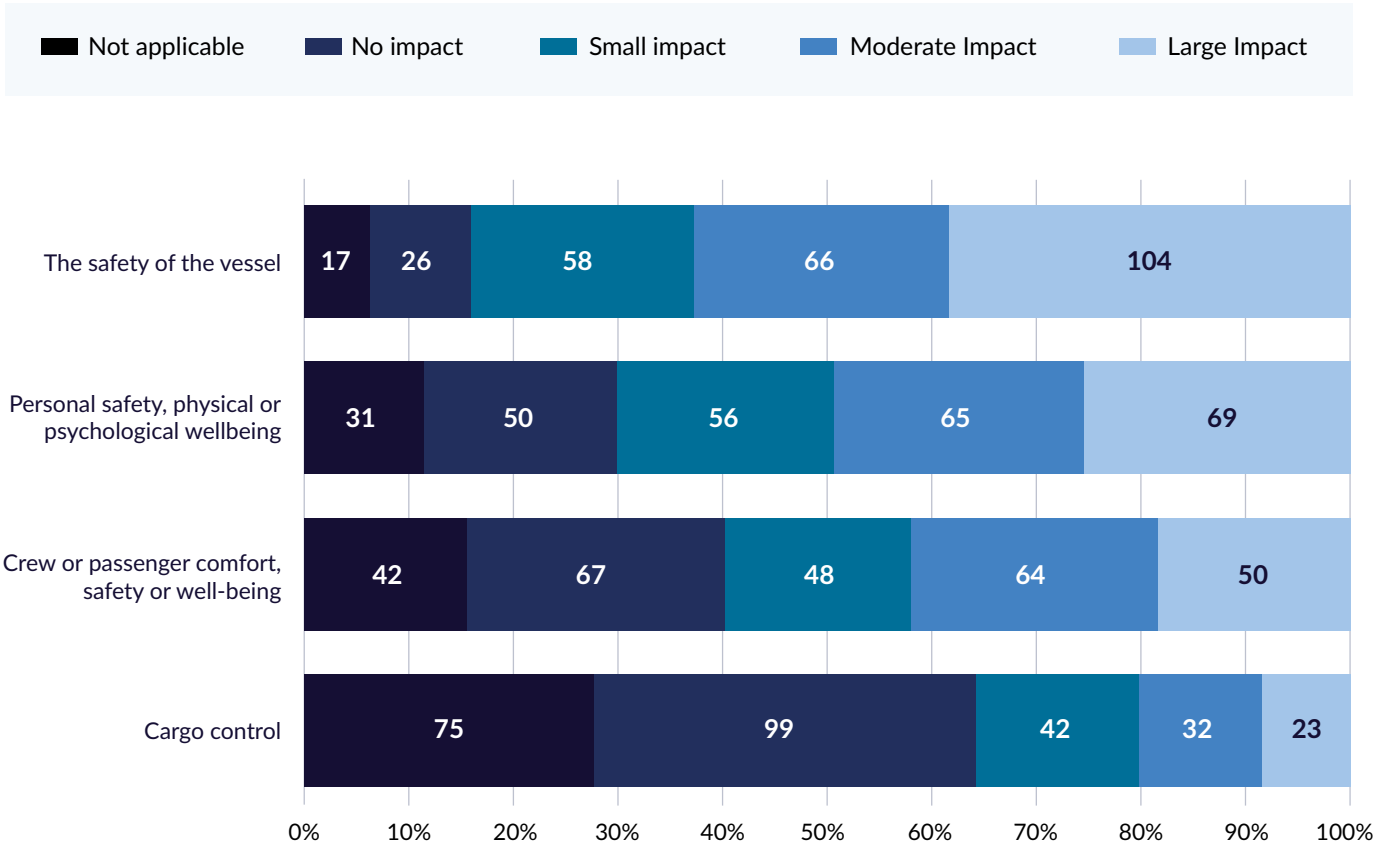


Figure 3.10 shows the impact that the GNSS interference has on various aspects of vessel, crew and cargo control.

Of significant concern is the revelation that 14% of respondents reported that GNSS interference had led them into an unsafe or unlawful situation. The survey also revealed that 8% of respondents had experienced physical harm to personnel related to GNSS interference, 8% reported property damage, and 4% reported environmental harm.

86% of respondents reported a moderate or significant concern that GNSS interference impacted safety.

From a technical standpoint, it is important to fully power cycle a GNSS receiver once the GNSS interference has ended, in order to completely clear its memory of all incorrect data. It was reassuring to see in the survey results that the vast majority of respondents (>80%) know how to do this and are willing to do so. However 7% reported that they are not permitted to do this.

42% of respondents reported that GNSS interference has reduced their trust in their vessel/systems.

Training and support

For 18% of those surveyed, they have not received training to avoid, detect or manage the GNSS interference, and 46% reported that their training was only informal or based on experience.

For those who had received formal training, 26% were at a maritime school, 20% used an online course, and 30% was mandated by their company.

30% of respondents were confident that the training they received helps them to mitigate against GNSS interference.

On the topic of additional support, 67% of respondents would like a warning before entering GNSS interference regions, 50% desire better equipment, 40% would like an alarm system, 35% would like to be able to isolate GNSS from other digital systems, and 22% reported a desire to know how to and be permitted to reset their GNSS receiver.

What additional **support** would you like to receive? (Select all that apply.)

258 responses

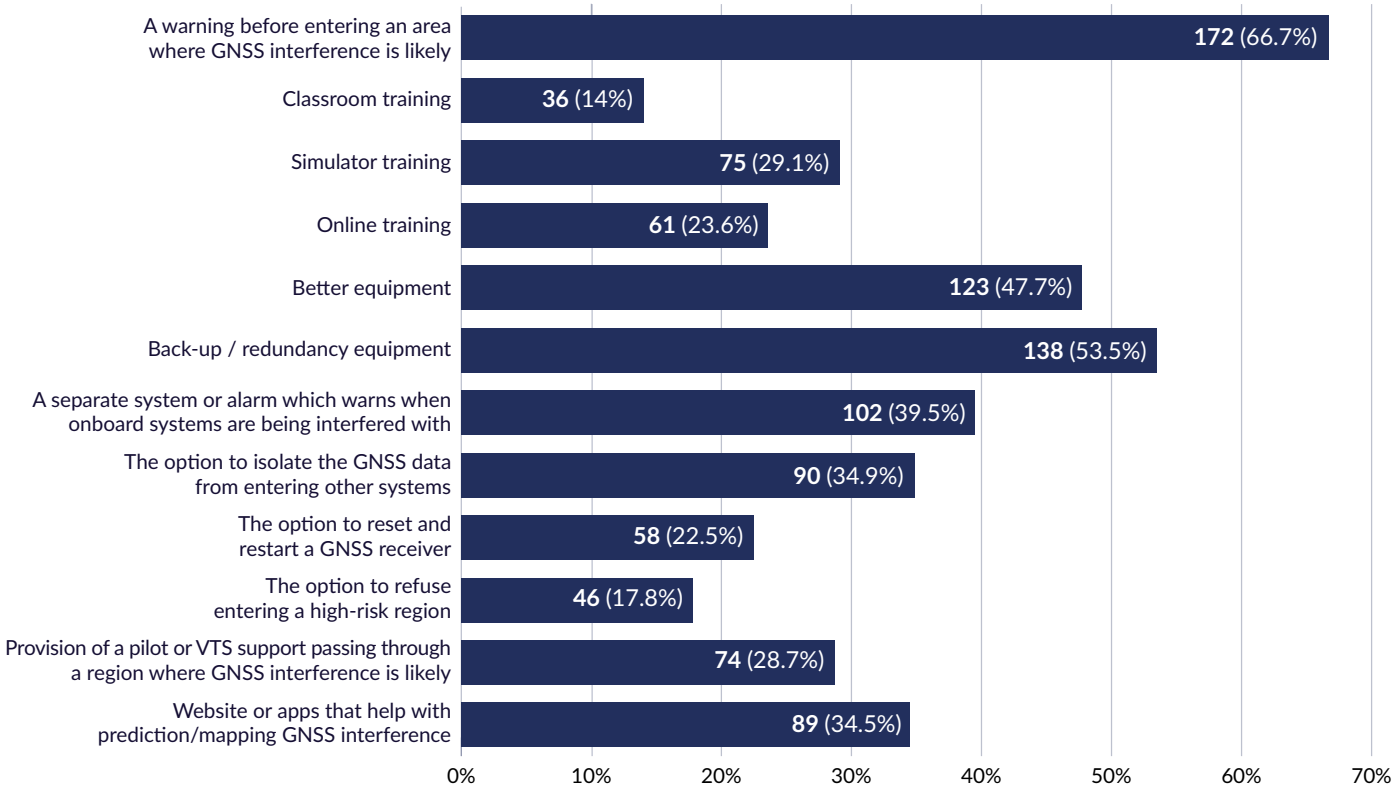


Figure 3.11 shows the types of additional support that survey respondents would like to receive when having to transit GNSS interference regions.

4

GNSS Connectivity Plot and Impacts of GNSS Interference on a Modern Vessel

A GNSS connectivity plot is a diagram that encapsulates all of the subsystems within a given system that can process GNSS-derived position, time or other data. Figure 4.1 shows an example diagram for a typical modern digital vessel. Depending on the exact make and model of various systems, GNSS data may or may not be processed, and it is strongly advised that vessel owners and operators establish their own GNSS connectivity plot for their own vessels and use them to understand their own vulnerabilities to GNSS interference. Assessments should be performed at a subsystem level by carefully checking the manuals for each digital system to confirm if GNSS/GPS data is processed or not. It is especially important to determine which systems have their own inbuilt GNSS receiver, and how this feature can be disabled or limited when encountering GNSS inference regions. This connectivity plot assumes a modern and fully integrated vessel operating in the open ocean (GMDSS Sea Area: A3/A4) and all the systems it COULD have which may include receiving a GNSS signal or have an in-built GNSS receiver. This will vary between vessels.

Mariners can navigate manually using traditional non-digital means such as a magnetic compass, a sextant, binoculars[12], etc, but their personal navigation skills cannot bring a satellite communications system back online or fix a jammed NAVTEX receiver.

This chapter discusses these connectivity issues and highlights the problems that can result from them during GNSS interference. In some examples these digital systems will be connected to the main GNSS receiver on the vessel that also feeds the navigation systems. In other examples these systems have their own GNSS receiver built into them, often as a "nice to have" or even a "premium" feature in a system which in reality does not require specific connection to a GNSS data input, and could instead derive position, velocity or time from a less vulnerable system.

The reason for such serious and wide-ranging problems with the sheer number of systems that process GNSS data is that GNSS is by far the cheapest and easiest way to provide a mobile platform with synchronisation to the Universal Time Coordinate (UTC, the internationally-recognised global time reference), and to determine position to accuracies of a few metres and velocities to accuracies of better than 1 ms^{-1} anywhere outdoors. However, modern society has become overly-reliant on open GNSS signals with no authentication or encryption to provide any security as to the authenticity of these positions, velocities and times.

The key emphasis of this chapter is that we demonstrate the sheer scale of the cybersecurity problem that manifests during GNSS interference. Less than half of the systems discussed below are navigation systems, and yet they are all at risk of malfunction or outputting incorrect information during GNSS interference. This is a serious and significant concern which must be addressed urgently. Mariners can navigate manually using traditional non-digital means such as a magnetic compass, a sextant, binoculars[12], etc, but their personal navigation skills cannot bring a satellite communications system back online or fix a jammed NAVTEX receiver.

[12] Noting SOLAS Ch V reg. 19 requires ships to have a magnetic compass, other navigation tools are not mandated.

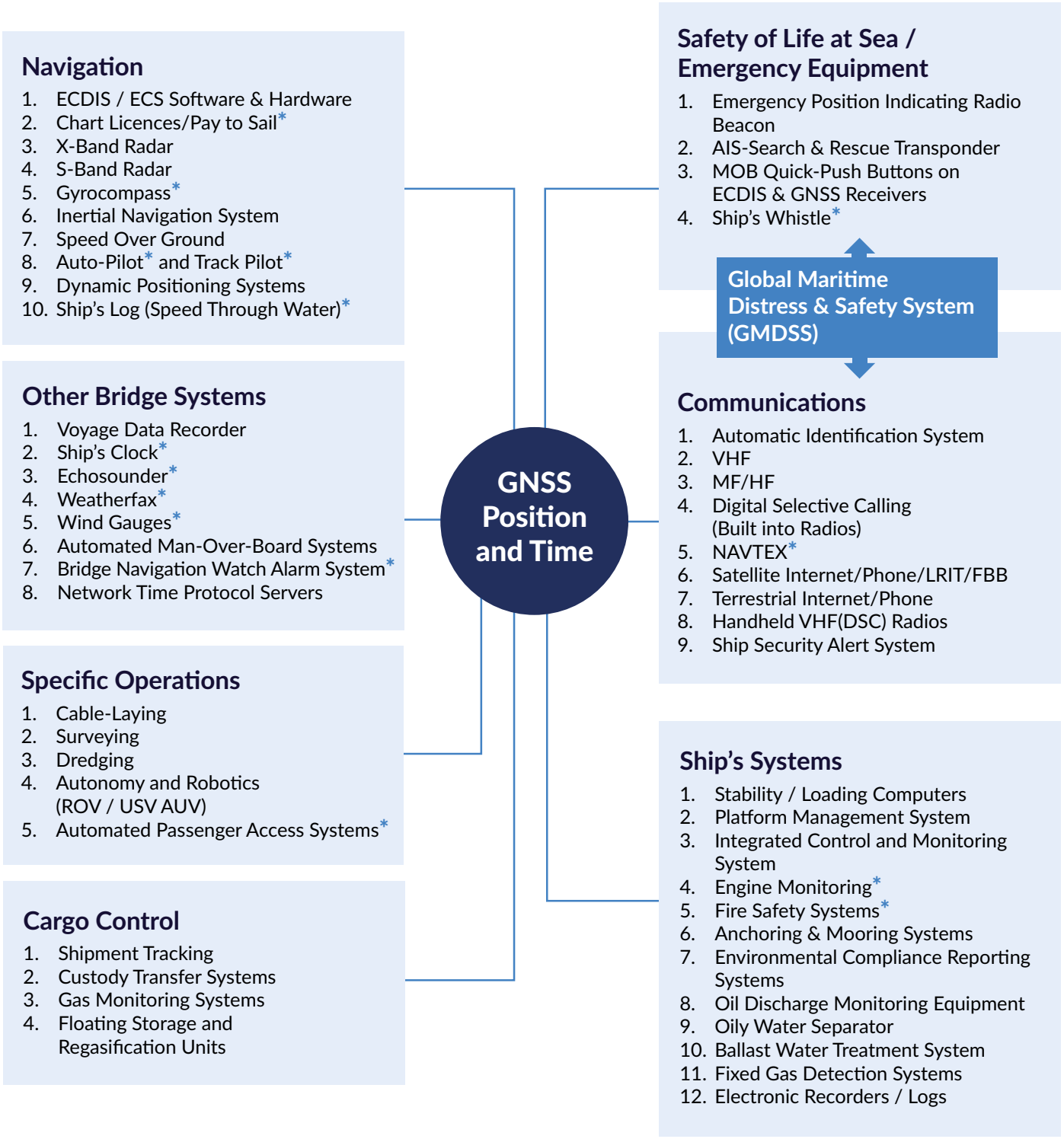
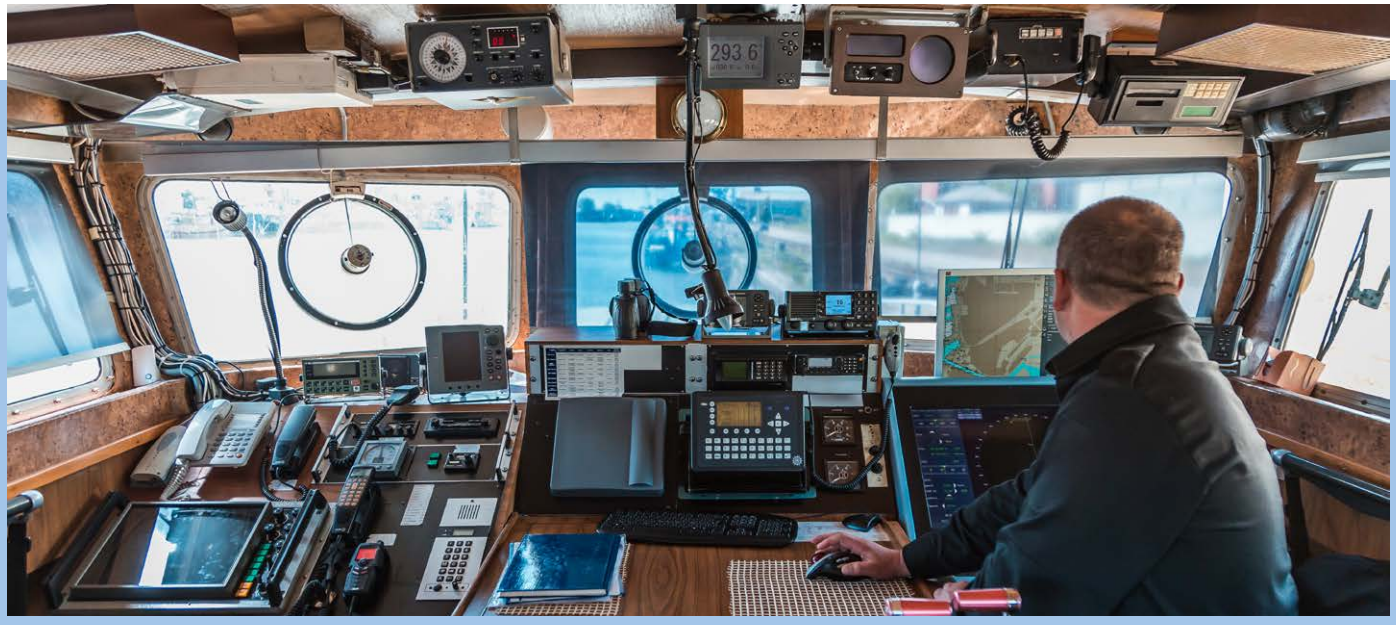


Figure 4.1 This GNSS connectivity plot shows the sheer scales of the issue with GNSS connectivity on a modern maritime vessel. There can be over 20 systems across 7 categories that process GNSS data or time, with less than half of these systems being associated with the navigation of the vessel.

Navigation Systems



There are various navigation systems onboard a modern vessel that use GNSS data for position, velocity and time. The GNSS receiver installed for navigation purposes feeds the ECDIS or electronic chart systems, and can also provide periodic updates to other navigation aids such as the gyro or an INS (inertial navigation system).

These other navigation systems that could be independent from GNSS, and indeed are assumed to be a backup during GNSS denial, can in some cases themselves be “polluted” by bad GNSS data during GNSS spoofing encounters.

From the survey results, interviews and studying hardware specification sheets, it is clear that systems such as the RADAR and the gyro can process GNSS data, sometimes using an internal GNSS receiver that cannot be disabled via any settings menu or by disconnecting a dedicated antenna. The problems that can arise in the worst case scenarios are that GNSS jamming can cause these dependent systems to cease to operate properly, and GNSS spoofing can result in these systems being put into degraded states, where their outputs are inaccurate, or unreliable.

GNSS Receivers

The vulnerability of GNSS receivers to GNSS interference is highly variable. Some older receiver designs still in use in the maritime sector today are easily jammed and spoofed, while the most modern receiver designs may contain specific anti-spoofing algorithms. Some GNSS-spoofing guidance materials published in the maritime sector in recent years recommend multi-constellation and multi-frequency receivers as a form of protection against jamming and spoofing. This, however, is not a robust solution if you are encountering active and intentional GNSS interference. *It is a dangerous assumption to make that the bad actor is able to interfere with some open GNSS signals and not others; it is much safer to assume that all open GNSS signals in that interference region are potentially compromised and that GNSS data should not be processed until the vessel is well clear of the interference region.* Exceptions to this are when known strong protections against GNSS interference have been installed for some receivers but not others, such as CRPA (discussed in Section 6).

The ESA Galileo constellation broadcasts the new OSNMA[13] (Open Service Navigation Message Authentication) which can be used by compatible receivers to provide an alarm that you have entered a spoofing region (if attempts are made to spoof the Galileo signals that are OSNMA watermarked). The new LEO constellation being built by XONA is also aiming to provide an authenticated ranging signal[14].

Effects of GNSS interference

The effects of GNSS interference on GNSS receivers is to deny their service and in the worst cases to cause them to confidently-output incorrect data, including position, velocity and time. In some cases interference can cause receivers to stop working (and require a power cycle) or can "brick" them completely. The survey results suggest that around 25% of the time when a GNSS receiver has suffered GNSS interference in the maritime sector, some manual intervention is required to return it to normal functioning (e.g. changing settings, resetting, power cycling, etc). The survey suggests that only around 2% of the time GNSS receivers have needed software or firmware to be replaced to return to normal functionality. The survey suggests that around 12% of the respondents who have noticed their GNSS receiver to be malfunctioning, noticed specifically that the time displayed was incorrect. There is a dedicated section on the Survey results below (Section 3).

[13] https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma
[14] https://arxiv.org/html/2510.02196v1

Effects of human interventions

There is little that can be done to a GNSS receiver in terms of changing settings or inputting information that can prevent jamming or spoofing from occuring. It is very important that a GNSS receiver that has suffered spoofing is fully power cycled once the vessel has left the GNSS interference region in order to fully clear all of the fake (spoofed) orbital data and other key parameters from memory. This is explained in more detail in Section 5 below.

ECDIS (Electronic Chart Display and Information System)

The ECDIS and other electronic charting systems replace the traditional paper charts used for maritime navigation, or are sometimes used alongside paper charts. The ECDIS processes data from GNSS receivers to show the vessel's current navigation solution.

Effects of GNSS interference

During GNSS interference ECDIS can exhibit various degraded states, including becoming difficult to use without manually disabling the GNSS input by adjusting the settings (e.g. GNSS spoofing can cause the displayed position to change rapidly as the spoofed GNSS position rapidly varies). The operator is required to understand how to put their ECDIS into different modes in order to ignore the incorrect GNSS data. The survey suggests that around 20% of the time when a GNSS receiver has suffered GNSS interference in the maritime sector, some manual intervention is required to return it to normal functioning (e.g. changing settings, resetting, power cycling, etc). The survey suggests that only around 1% of the time has the ECDIS needed software or firmware to be replaced to return to normal functionality.

Effects of human interventions

Changing the settings on ECDIS and other electronic charting systems can isolate the systems from GNSS inputs, and resetting the ECDIS completely can be a last resort to removing the effects of GNSS spoofing that may have corrupted data in an ECDIS. It is highly recommended that mariners ensure they are aware of how to set their ECDIS into modes that isolate it from GNSS data. If the time displayed on the ECDIS is incorrect when compared to a traditional analogue wristwatch (not a smartwatch containing a GNSS chip) this is a clear indicator that spoofed GNSS data has infiltrated the ECDIS.

Chart Licences

Paper charts have largely been replaced by electronic displays, and these systems display charts that are purchased under licence, sometimes automatically as vessels move into new regions and therefore require new charts.

Effects of GNSS interference

During GNSS interference the time calculated by GNSS receivers can be far into the past or future. This can cause digital licences to expire, and so can cause charts to “disappear” from electronic systems accordingly. Since GNSS interference can also cause vessels to believe they are in completely different locations, charts may automatically be purchased on these systems unnecessarily for locations that the vessel has not, and will not, enter into.

Effects of human interventions

It is highly recommended that mariners ask their system providers how their chart licensing system sources position and time, and to understand what is expected to happen if the time and date are spoofed far into the future or past. The mariners should also disable any auto-purchasing features of their electronic charting systems when expecting to encounter GNSS interference.

RADAR

RADAR provides critical situational awareness by confirming the range and relative bearing and speed of other objects in the vicinity, thereby allowing the mariner to take early action to avoid collision. Navigation in littoral waters is achieved by using planned distances and bearings from distinct points of land or other stationary objects and, on more modern equipment, can be overlaid on an electronic charting system to verify position and the accuracy of other inputs (e.g. gyro and any RADAR equipment offsets). This is in addition to using multiple RADAR ranges as a position fix.

Effects of GNSS interference

Unfortunately, even though 87% of the respondents stated that they rely on the RADAR position-fixing capability to help them to determine that GNSS interference has ceased, the survey revealed that 50% of the respondents have observed their RADAR to exhibit problems during GNSS interference. The survey also revealed that around 16% of the time that the RADAR suffers from GNSS interference, manual intervention has been required in order to resume its functionality after leaving the interference region (e.g. changing settings, resetting, power cycling, etc).

While it may seem surprising that RADAR systems can be dependent on GNSS data, this vulnerability has been known for a very long time[15]. While the transmitting and receiving of high powered RADAR pulses by a transceiver

[15] General Lighthouse Authorities of UK & Ireland, "GNSS Jamming Trials Report", 2008

can be achieved independently of GNSS, in a modern integrated RADAR systems GNSS data is often used later in the signal processing chain to provide position, speed-over-ground and heading, in order to provide anti-collision, ground stabilization, chart overlay and true motion display modes. Such features are lost if the GNSS data is unavailable, and the operator may need to change various settings on the RADAR to overcome these issues or to silence alarms.

Effects of human interference

On entering an area of GNSS interference, if the Automatic RADAR Plotting Aid (ARPA) functionality is lost due to a loss of position, speed or heading input from GNSS, the RADAR can still be used to assess the range and bearing of objects or vessels in the vicinity by switching modes. These changes are likely to include switching from “speed over the ground” (SOG) input to “speed through the water” (STW) input; switching from ground stabilisation to sea stabilisation mode; and monitoring relative bearings after switching to head-up mode.

Gyrocompass

A gyrocompass can determine the direction of True North when it is stationary, by directly measuring the axis of rotation of the Earth. However when a gyroscope is mounted on a vessel that is moving great distances, an error term manifests in this estimate that depends on both the vessel’s latitude and its velocity. To compensate for this, a moving gyroscope needs to be provided with the current latitude and velocity, these are then used to calculate the required heading correction to the gyroscope output. In many modern commercial gyrocompasses, the estimates of latitude and velocity are typically provided by a GNSS receiver.

Effects of GNSS interference

If the gyroscope is provided with latitude and velocity directly from a GNSS data feed, then during GNSS interference these values can be incorrect, resulting in an incorrect heading correction, and therefore an incorrect output heading from the gyrocompass. During extended jamming periods, the loss of all GNSS data would result in the gyrocompass accuracy gradually degrading as its estimate of North drifts due to the lack of accurate Latitude and velocity updates. During GNSS spoofing the “confidently wrong” Latitude and velocity data being passed to the gyrocompass would degrade its accuracy much more rapidly than if it were simply disconnected entirely from the GNSS data. Some gyrocompasses may incorporate anti-spoofing logic to detect and ignore incorrect GNSS data rather than simply accept and process it.

Effects of human interventions

The GNSS feed to the gyro should be disabled before entering a region of GNSS interference, else the gyro may need to be reset/rebooted after leaving the GNSS interference region to ensure that any incorrect data has been removed from its memory. In the survey, 38% of the respondents reported issues with their gyro during GNSS interference, with 8% reporting that the gyro continued to behave incorrectly after leaving the interference region. The survey suggested that the gyro needs a physical intervention by a crew member to ensure its full recovery 25% of the time after encountering GNSS interference.

Inertial Navigation Systems

Modern Inertial Navigation Systems (INS) are integrated with GNSS receivers as their primary source of assistance and correction data. Not all ships use an INS.

Effects of GNSS interference

Providing an incorrect GNSS position and/or velocity to an Inertial Navigation System can result in unrecoverable disruption to the INS position and velocity output, requiring reinitialisation. Extreme GNSS errors should be ignored by a well-designed INS, but subtle spoofing errors may successfully pollute an INS. It is possible that the “crop-circle” spoofing attacks are designed to try to capture and disrupt INS. It is also possible that most INS have not been tested for their behaviour when exposed to GNSS time jumping forwards or backwards, as is often the case during GNSS spoofing.

Effects of human interventions

Disconnecting the GNSS feed prior to entering a GNSS interference region is a possible measure that could be taken to protect the INS from accepting false GNSS information during GNSS spoofing. Well-designed INS should offer robustness against GNSS jamming and spoofing, but their accuracy will always degrade over time and distance whenever correction measurements are unavailable.

Speed Over Ground

Speed over the ground (SOG) refers to the vessel’s speed relative to the Earth’s surface. Unlike speed through the water (STW), which is a measure of the vessel’s velocity through the moving body of water, SOG is an essential metric in marine navigation because it accounts for the actual

distance covered over time and is a much better measure for performing dead reckoning than STW.

Effects of GNSS interference

SOG is typically provided to a modern vessel via a GNSS receiver, and so can be unavailable during GNSS jamming and can be wildly inaccurate during GNSS spoofing.

Effects of human interventions

Speed over ground can be calculated via other means if they are available, such as eLoran or other radio navigation aids, or by altering the Doppler Log to use a bottom-track mode.

Speed Log / Doppler Log / EM Log

The speed log provides the speed through the water (STW) measurement, often using Doppler (acoustic measurements) or EM (Electromagnetic) sensing. STW is the input which should be used when monitoring a RADAR for the purposes of anti-collision, when determining the relative course and speed of another vessel moving in the same body of water.

Effects of GNSS interference

The Doppler Log is a clear example of a piece of technology which has no primary need to be connected to GNSS in order to provide its critical function. However many modern Doppler Logs use GNSS data to provide a calibration/correction to estimate Speed over Ground from Speed Through Water. The survey has revealed that the Doppler Log is affected by GNSS interference for 21% of the respondents. The respondents also reported that they noticed the date or time to be incorrect on the Doppler Log 33% of the time during GNSS interference. Some Doppler Log systems may also make use of GNSS time in order to ensure their measurements are synchronised well with other parts of the navigation system.

Effects of human interventions

Doppler Logs with no dependency at all on GNSS are recommended. Mariners should establish how to disable any GNSS input to their Doppler Log before entering a GNSS interference region. The survey suggested that Doppler Log would recover on its own after GNSS interference 92% of the time, for the other 8% some manual resetting was required.

Autopilot and Track Pilot

The autopilot is designed to steer a fixed heading and relies on a variety of sensor inputs, including gyro heading and the ship's speed. Many modern autopilots also process GNSS data.

Effects of GNSS interference

During GNSS interference an autopilot that depends on GNSS will trigger an alarm that GNSS/speed/position is unavailable (jammed), although during spoofing there is a risk that the autopilot could incorrectly manoeuvre the vessel and will need to be manually disabled. This behaviour has been reported by mariners that completed the survey. In the survey, 32% of respondents reported that the autopilot is adversely affected during GNSS interference, with the data further suggesting that 25% of the time, these disrupted autopilots require manual intervention in order to recover the autopilot's normal functionality after leaving the GNSS interference region.

Effects of human interventions

For autopilots that are known to alarm and to be susceptible due to GNSS interference, these systems should be disconnected from GNSS or disengaged completely before entering GNSS interference regions, where possible.

Dynamic Positioning Systems

A dynamic positioning system is designed to maintain both a ship's heading and its position. As such, the control system operates the rudders, engines and thrusters. These systems are most commonly found in vessels conducting special operations, such as cable-laying, surveying and offshore support and supply vessels.

Effects of GNSS interference

There are three classifications of Dynamic Positioning System, according to the IMO, which correspond to their capabilities and system redundancy. However, all three require an accurate position source and a loss of GNSS may trigger an alarm and could in some cases result in the vessel moving out of position and requiring manual intervention. Failure of the dynamic positioning system within GNSS interference regions were specifically described by 4 of the survey's respondents. One respondent reported "[Our] Dynamic Positioning system can be affected when [GNSS] jamming or spoofing is active. However, with anti-jamming antennae installed, there have been instances where nearby vessels' D-GNSS systems were rendered unusable while our D-GNSS systems remained usable". A different survey

respondent reported their DP equipment being inherently robust to the interference: “As a construction vessel our DP systems and survey gear use separate GNSS receivers which are more accurate and less susceptible to spoofing than the IMO approved equipment. However since they are not IMO approved we cannot use them for navigation. All the traditional navigation equipment was completely knocked out while our survey gear remained mostly accurate. During peak events the units with vector option were the most reliable.”.

Effects of human interventions

Where the use of a DPS is required for an operation in an area of known GNSS interference, system operators must be familiar with all its modes of operation and actions to be taken in the event of a failure due to GNSS jamming or spoofing. All operations should be appropriately risk assessed and particular attention should be taken in high-risk environments, especially if conditions worsen.

SOLAS (Safety Of Life At Sea) Systems

The International Maritime Organisation's International Convention in the Safety of Life at Sea mandates that certain equipment must be carried by vessels. SOLAS vessels are ships, from large cargo carriers to smaller commercial yachts, that must comply with SOLAS, an international treaty setting minimum standards for ship construction, equipment, and operation to protect life at sea. While primarily for ships on international voyages, certain SOLAS rules, especially Chapter V on navigation, apply broadly, even to private pleasure craft, mandating standards for radio, distress signals, voyage planning, and more. Of particular concern in the connectivity plot is the number of SOLAS mandated systems that use GNSS data. This list includes GMDSS, EPIRB (Emergency Position Indicating Radio Beacon), AIS-SART, MOB (Man OverBoard) quick-push buttons, and even the Ship's Whistle.

In the case of GMDSS, EPIRBS, AIS-SART and MOB buttons these technologies all fundamentally involve a position fix (and in some cases a time) being transmitted over a radio link, and will be referred to below as "Emergency Beacon" technologies.

Emergency Beacon Technologies (GMDSS, EPIRB, AIS-SART and MOB buttons, etc)

Effects of GNSS interference

Many emergency beacon technologies in use in Maritime have a heritage that predates GNSS, and in many cases still use legacy technologies where possible. A good example of this is EPIRB, which transmits a distress message on 406 MHz when activated, and a constellation of COSPAS/SARSAT satellites in orbit detect and geolocate this signal. However the time taken to calculate this position is much slower (many minutes) and lower in accuracy (many hundreds of metres) than for a GNSS fix (metre-level accuracy calculated within 30 seconds or less). For these reasons, modern devices all broadcast a GNSS position fix over the 406 MHz emergency channel in order to provide a faster and more accurate position during the distress call. However the issue in GNSS interference regions is therefore very clear: in some circumstances where GNSS is jammed, then this extra situational awareness information will be unavailable during an emergency. Much more concerning is the issue that during GNSS spoofing the position provided over EPIRB is expected to be incorrect, potentially sending any rescue team to the wrong location to attempt to rescue those in distress.

Technologies such as AIS-SART are entirely dependent on GNSS positioning for the emergency location, and use AIS to broadcast the distress call, which itself is known to also be intentionally interfered with in the modern threat landscape (see Appendix A for a discussion of AIS). These particular devices should therefore not be relied upon at all to function in the intended manner when undergoing GNSS interference.

It is highly recommended that any safety systems that incorporate GNSS be tested thoroughly in both jamming and spoofing test environments to confirm how they behave, and if they do not behave as required that the manufacturers urgently provide replacement systems or software updates. The concerns are potential failure modes such as:

- During barrage GNSS jamming, the emergency system does not correctly provide a desired emergency broadcast containing minimum required information.
- During GNSS spoofing where time & date are incorrect, the emergency system does not correctly provide a desired emergency broadcast containing minimum required information.
- During GNSS spoofing the emergency system broadcasts incorrect position over the radio link which is not successfully overridden by any other (lower accuracy) position fix that the system is capable of generating.

- Following GNSS interference the emergency system is left in a degraded mode or inoperable state (requiring manual resetting or complete replacement).

There is no "single answer" to the above set of questions since there are so many different manufacturers and models of various systems in use, and so testing is required to establish the vulnerability (and its remedy) for each case.

In the case of AIS SART, it is recommended that other SOLAS systems are also provided alongside these beacons when operating in areas of GNSS interference. It should be noted that often RADAR SARTs are paired with AIS SARTs but a concern here is that our survey has revealed that issues with RADAR are experienced around 50% of the time when vessels are operating within GNSS interference regions. In a worst case scenario, during GNSS interference an AIS SART may be providing a wildly incorrect position estimate, and a rescue vessel's RADAR may also be experiencing associated GNSS interference issues at the same time.

At the time of writing it is not clear to the authors where the liability lies in situations where SOLAS systems are negatively impacted in certain regions of the world, and this information is known to the mariners and vessel operators in advance. In other words - what are the liability issues associated with chartering a vessel to transit a known GNSS interference region, when it is known that the safety systems onboard that vessel are likely to be compromised while in that region. Similarly, it is not clear at this time to the authors as to impact on insurance claims if a vessel is lost, cargo is lost, or lives are lost in these particular circumstances.

Around 14% of respondents reported that their SOLAS systems are adversely affected during GNSS interference, with the data further suggesting that 9% of the time, these disrupted SOLAS systems require manual intervention in order to recover their normal operations after leaving the GNSS interference region. It is important to note however that the various SOLAS systems distributed throughout a vessel are not as conspicuous to the captain and other crew as systems alarming on the bridge will be. It is possible therefore that the proportion of SOLAS systems negatively impacted during and after encountering GNSS interference regions will be much higher than this. In the survey, 45% of respondents reported that the GMDSS systems are adversely affected during GNSS interference, with the data further suggesting that 15% of the time, these disrupted GMDSS systems require manual intervention in order to recover their normal operations.

Around 14% of respondents reported that their SOLAS systems are adversely affected during GNSS interference.

Effects of human interventions

In some SOLAS systems it may be possible for the human operator to deselect GNSS when entering an area of GNSS interference, or to manually input position information periodically (for example this is possible on GMDSS). It will be important for the crew to have available a specific checklist for their SOLAS systems when entering and leaving GNSS interference regions if they need to temporarily put these systems into specific modes.

Some systems cannot be provided with any external information on position or time, for example AIS-SART systems cannot be provided with any other position information except for their built-in GNSS receiver. This is a serious problem that cannot be overcome by the mariner's personal navigation skills and access to alternative positioning technologies and techniques. Fundamentally the mariner's skills with a sextant are irrelevant if they fall overboard wearing an AIS-SART within a GNSS interference region. Their safety is entirely at the mercy of GNSS interference at that point if alternative GNSS-independent SOLAS systems are not available to them.

Ship's Whistle

In fog or restricted visibility, ships are required by the International Regulations for Preventing Collisions at Sea (COLREGs) to sound specific, usually automatic, whistle or foghorn blasts at regular intervals to communicate their presence and status to other vessels. The exact pattern of blasts required depends upon various criteria such as: power-driven vessel making way through the water, power-driven vessel underway but stopped (not making way), vessels not under command, restricted in ability to maneuver, sailing vessel, or towing another vessel,and vessels at anchor. In some modern systems targeting the yachting sector, the ship's whistle in fog functionality can be provided by the VHF/DSC connected to GNSS in order to automatically select the correct blast patterns[16]. The Ship's Whistle is a good example of hardware which does not require any GNSS data in order to perform its primary function, and yet, at least in the pleasure-boat community, GNSS connectivity is in some cases being added to even these simple components.

Effects of GNSS interference

A ship's whistle connected to GNSS data in order to select the correct whistle sounding pattern based on the motion of the vessel may not operate properly during GNSS interference. The complete absence of GNSS data due to jamming may result in the whistle not sounding correctly, or at all.

[16] https://www.yachtingmagazine.com/uniden-525-dsc-vhf-and-jensen-speaker-system/

The impact of GNSS spoofing potentially placing the estimated position of the vessel well outside the region of fog could result in the system not sounding any blasts at all while in fog. It is highly recommended that the behaviour of any integrated ship's whistles that are connected to GNSS data be tested for the various behaviours under different types of GNSS interference. The concerns are potential failure modes such as:

- During barrage GNSS jamming, the ship's whistle does not provide the correct blasts during fog.
- During GNSS spoofing where time & date are incorrect, the ship's whistle does not provide the correct blasts during fog (e.g. due to a software issue caused by big time jumps).
- During GNSS spoofing the incorrect position estimate results in no whistle blasts being broadcast while the vessel is in fog.
- Following GNSS interference the automated feature of the ship's whistle is left in a degraded mode or inoperable state (requiring manual resetting or complete replacement).

It is highly recommended that the behaviour of any integrated ship's whistles that are connected to GNSS data be tested for the various behaviours under different types of GNSS interference.

There is no "single answer" to the above set of questions since there are so many different manufacturers and models of various systems in use, and so testing is required to establish the vulnerability (and its remedy) for each case.

Effects of human interventions

The ability for the human operator to override or correct the erroneous GNSS information being processed by the Ship's Whistle during periods of GNSS interference will be dependent on the features provided on a given make and model of Ship's Whistle. It will be important for the crew to have available a specific checklist for their Ship's Whistle when entering and leaving GNSS interference regions if they need to temporarily put these systems into specific modes if they also encounter restricted visibility within the interference region.

Communications Systems

Satellite Communications

Satellite communications (SATCOM) transceivers often incorporate their own GNSS receiver to accurately determine position, frequency and time. In some cases GNSS is used to physically point a movable dish at the SATCOM satellite or direct the beam steering of an array of antenna elements. In those cases, the effect of misspointing will depend on how directional the antenna is and how high the frequency used is (and therefore, how narrow the bandwidth).

Effects of GNSS interference

GNSS spoofing of position and time can have a number of serious impacts on a satellite communications system, such as:

1. Depending on the communications protocol, the handovers from satellite beam to beam might depend on the GNSS position and time, or might be driven by signal strength of the different beams. In the former case, an incorrect (spoofed) GNSS position and time can cause delayed or premature handovers into beams that don't provide good coverage for the terminal's spoofing location, resulting in worse performance (signal to noise ratio and throughput) for the terminal, but also more interference to non adjacent beams that share the same frequency. In the worst case scenario, powering up a SATCOM system while undergoing GNSS interference may cause the satcom terminal to be unable to acquire service at all, due to the same issues of searching incorrectly for a serving satellite.

2. A spoofed GNSS position may also impact the regulatory limitations on the spectrum that the terminal can use, or whether it is allowed to operate at all. In this worst case example, a SATCOM terminal is spoofed for a geographical location where it is not permitted to be used and so it ceases to function (while actually in a location where it is permitted). An erroneous position could result in a terminal using spectrum allowed in the spoofed-to position that it shouldn't be using in its spoofing location, interfering with the legitimate users of that spectrum.

3. A spoofed GNSS position may result in the SATCOM terminal using spectrum that is not permitted in its true location, or suboptimal and resulting in poor communications performance and congestion. Behaviour here will vary between systems with hard beam boundaries, and systems with beam overlaps which employ load balancing. The load balancing in overlap areas should prevent some of the congestion build up.

4. A spoofed time that is far into the past or the future can cause issues that will disrupt the correct operation of a satellite communications transceiver[17].

5. Of particular concern are systems where distress calls can be automated with a "red button" functionality on the terminal, and during GNSS interference this distress call could include incorrect vessel location, and/or incorrect date and time associated with the distress message. As distress calls will have the highest priority, in a scenario of GNSS interruptions increasing congestion and worsening network performance but not causing a full outage, the distress call should still successfully propagate through the network.

6. The Long-Range Identification and Tracking (LRIT) messages being created by a given vessel every 6 hours and broadcast via satcoms will contain incorrect positioning data during GNSS spoofing.

The survey suggested that 39% of respondents have experienced issues with SATCOM during GNSS interference, with the SATCOM systems requiring manual intervention (changing settings, or rebooting, etc) in order to return to normal operations after leaving the interference region in 32% of the cases.

The survey suggested that 39% of respondents have experienced issues with SATCOM during GNSS interference.

Effects of human interventions

Humans can attempt to reboot and reset SATCOM systems after leaving GNSS interference regions in order to return to normal functionality, but for most SATCOM systems that rely on an internal GNSS receiver for their operation, there will be no way for a human operator to override or correct this incorrect GNSS data. A satcoms unit that takes an external GNSS input could however benefit from being fed data by a "master" GNSS navigation receiver with anti-interference capabilities (e.g. connected to a CRPA).

AIS (Automatic Identification System)

The AIS provides a situational awareness capability by sharing GNSS position fixes (and other information such as identity) over a simple radio link at 162 MHz. However neither the AIS radio link, nor the traditional GNSS signals incorporated, employ any authentication or encryption capabilities. As such, it is straightforward to broadcast fake AIS signals, and it is also the case that within GNSS interference regions, spoofed GNSS positions are shared over the AIS link (displaying vessels in incorrect locations on AIS screens). These issues with AIS are discussed in Appendix A.

[17] https://www.jrc.co.jp/en/news/2024/0821-1

Effects of GNSS interference

During GNSS jamming there are no GNSS fixes available to share over AIS. During GNSS spoofing a spoofed GNSS receiver will share an incorrect position fix over the AIS radio link.

The survey suggested that 74% of respondents have experienced issues with AIS during GNSS interference, with the AIS systems requiring manual intervention (changing settings, or rebooting, etc) in order to return to normal operations after leaving the interference region in 19% of the cases.

Effects of human interventions

AIS has been designed to be entirely driven by GNSS, and as such it is not common for AIS systems to be capable of taking alternative inputs for position. This is another example of the main issue not being specifically one where humans should be capable of navigating without GNSS, but rather an issue of cybersecurity challenges where automated systems are not just spreading incorrect information around a given vessel's electronic systems, but are also broadcasting those incorrect data to the whole world, reducing overall situational awareness and removing the use of a very useful automated safety system.

GMDSS (Global Maritime Distress and Safety System)

GMDSS has already been discussed in the SOLAS subsection above.

VHF/MF/HF

These radio technologies are well established traditional communications systems in the maritime sector. These are clear examples of systems on a modern bridge which should not require GNSS connectivity in order to provide their primary function, but in all cases there are examples where a modern radio system might have GNSS embedded within it for a "nice-to-have" or secondary feature. For example there are examples of radios that use an in-built GNSS receiver in order to simply display the time accurately on the display.

Effects of GNSS interference

In the case of these radio transceivers, those with Global Maritime Distress and Safety System (GMDSS) functionality incorporated will transmit GNSS derived position via Digital Selective Calling (DSC) on channel 70 VHF. Lower-cost and older VHF handhelds don't support DSC and while GNSS interference will affect the DSC messages it should not affect the analogue voice functionality on a simple handheld VHF radio but given the sheer scale of this GNSS connectivity problem, all devices should be checked for an internal GNSS receiver, and their potential failure in regions of GNSS interference noted accordingly.

The survey suggested that 37% of respondents have experienced issues with their radio sets during GNSS interference, with these systems requiring manual intervention (changing settings, or rebooting, etc) in order to return to normal operations after leaving the interference region in around 9% of the cases.

Effects of human interventions

With the exception of GMDSS, it is typically the case that any VHF/MF/HF radio that has an incorporated GNSS receiver as a "nice-to-have" feature will not have any external connectivity option to override that internal GNSS receiver. As such a misbehaving or failed radio set during GNSS interference may require manual resetting after leaving the interference region in order to restore its functionality. Without GNSS input, the user must manually enter an updated position at least every 4 hours on the GMDSS. However it is not clear during GNSS spoofing whether this overrides the incorrect GNSS data. It is likely that this will need to be tested/confirmed directly on all makes and models of these radios (it is unlikely to be part of the traditional testing of these devices before they were sold).

NAVTEX

NAVTEX (NAVigational TEXt) is an international, automated medium-frequency radio system that broadcasts crucial maritime safety information like weather forecasts, navigational warnings, and urgent alerts directly to ships as printed text, forming a key part of the Global Maritime Distress and Safety System (GMDSS). It operates on a schedule, primarily on 518 kHz for English messages, providing vital, real-time data for safe passage, especially beyond coastal VHF range.

Like VHF radio, the NAVTEX service itself doesn't depend on GNSS, but modern "premium" category NAVTEX receivers include additional GNSS functionality.[18] This is likely to provide features such as the display of time and date, the filtering/categorisation of messages by geographical proximity, position display, automatic station selection, etc. Maritime Safety Information can also be received via Recognised Mobile Satellite Service (RMSS) such as Iridium, Inmarsat, or SafetyNET rather than via NAVTEX.

It is a recommendation of this study that NAVWARNS broadcasts should be updated to include GNSS interference information.

It is a recommendation of this study that NAVWARNS broadcasts should be updated to include GNSS interference information. A modern weather report should include the current conditions for electronic interference in a given region.

Effects of GNSS interference

Since the provision of GNSS data is not a fundamental requirement for NAVTEX functionality, it is difficult to predict the scale of issue that GNSS interference might cause to a NAVTEX receiver with built-in GNSS receiver. Therefore thorough testing of any NAVTEX receiver with a built-in GNSS receiver is highly recommended. The concerns are potential failure modes such as:

- During GNSS jamming, the NAVTEX system does not correctly display or print out information it receives.
- During GNSS spoofing where time and/or date and/or position are incorrect, the NAVTEX system does not correctly display or print out information it receives.
- Following GNSS interference the NAVTEX system is left in a degraded mode or inoperable state (requiring manual resetting or complete replacement).

[18] https://www.icselectronics.co.uk/leisure/nav6

The survey suggested that 24% of respondents have experienced issues with their NAVTEX during GNSS interference, with these systems requiring manual intervention (changing settings, or rebooting, etc) in order to return to normal operations after leaving the interference region in around 9% of the cases.

Effects of human interventions

For NAVTEX systems with built-in GNSS receivers it is recommended that it is determined whether those features can be disabled (e.g. in a settings menu) prior to entering a GNSS interference region where necessary.

Effects of human interventions

For NAVTEX systems with built-in GNSS receivers it is recommended that it is determined whether those features can be disabled (e.g. in a settings menu) prior to entering a GNSS interference region where necessary.

LTE Connectivity to GNSS

Consumer LTE mobile telephones typically include GNSS receivers used for location apps. LTE functionality can be bundled into VHF handhelds and some manufacturers offer GNSS dependent mapping and geofencing.[19] If the position is spoofed in and out of a geofenced area, the users would be receiving SMS alerts for entering and exiting this area. The LTE network itself will depend on GNSS, using GNSS disciplined oscillators for time/frequency reference[20].

[19] For example VHF/LTE handhelds https://icomuk.co.uk/IP-M60-Hybrid-LTE/Handheld-VHF-Marine-Radio with mapping and geofencing functionality via https://icomuk.co.uk/RMS-IP-LTE-Radio-Dispatcher
[20] https://insidegnss.com/vodafone-turkey-adopts-advanced-timing-technology-for-network-resilience-gnss-disruptions/

Operational System Dependencies

Aside from the above critical systems that have been identified to process GNSS data for either primary or secondary functions, there are a plethora of other operational functions on a modern vessel that can also be connected to GNSS data for position or timing information. In each of the below cases, where a vulnerability is of concern, the recommended testing steps should consider as a minimum:

- During GNSS jamming, does the system operate normally, or as expected?
- During GNSS spoofing where time and/or date and/or position are incorrect, does the system operate normally, or as expected?
- After leaving a GNSS interference region, does the system return to normal operations without manual intervention?

Bridge Systems

Various systems such as Ship's Clock, VDR, Echosounders, Weatherfax, Wing Gauges, CCTV systems, BNWAS and many others may access GNSS data for "nice to have" features, the most typical being to timestamp their data or display.

The survey suggested that issues with the Ship's Clock had often been observed during GNSS interference, as noted by 19% of the respondents. The survey further suggests that the Ship's Clock would recover on its own after GNSS interference 74% of the time, else a manual intervention was required to return the Ship's Clock to its expected behaviour.

Vessel Systems

Various systems such as the stabilisers, engine monitoring system, fire safety systems, anchor & mooring systems, environmental compliance reporting, and any automated systems may be connected to GNSS data, or have a built-in GNSS receiver, to access position or date&time. For example some vessels may have a "white box" under MARPOL for overboard discharges, which may have a GNSS input to record vessel's position when discharging oily water, with oil content also recorded. This is considered to be proof that the vessel was legally discharging any oily water overboard, as it automatically records data, synchronising time/ position with oil content. Incorrect GNSS position or time could inadvertently cause illegal overboard discharging. Intentional GNSS spoofing could instead mask intentional illegal discharges.

It is recommended that operators provide a "systems audit" of their own to verify their vessel's specific connectivity diagram and where necessary establish the procedures that are required to protect the operation of their vessel during periods of GNSS interference.

Network Time Protocol (NTP)

The Network Time Protocol is used within computer networks to distribute and synchronise time. On moving platforms it is common for NTP servers to be regularly updated using GNSS. If the NTP server on a vessel is spoofed to the incorrect time, then this incorrect time can be distributed via NTP to all of the connected systems on the vessel. It is important to check the manual for a given GPS/GNSS disciplined NTP timing server for any information on spoofing detection or rejection, else to confirm directly with the manufacturer as to the expected behaviour.

Any systems onboard a vessel that is synchronised via NTP could become affected by GNSS spoofing of time in this manner if the NTP server is not robust to GNSS spoofing attacks. The list of connected systems onboard a vessel should be generated in order to assess what the vulnerabilities might be. In theory a wide variety of onboard systems may be connected via NTP, for example:

- Custody Transfer Systems into the Cargo Control section
- Oil Discharge Monitoring Equipment
- Ballast Water Treatment System
- Oily Water Separator
- Pilot plugs (Pilot portable devices)
- Satellite phones

- Cybersecurity services
- Fixed Gas Detection Systems
- Fire Alarm Main and Remote Panels
- Gas Custody Transfer Systems (Data Acquisition and Reporting)
- Gas Generator Alarm and Parameter Monitoring Systems
- Stability/Loading Computers
- Ballast Water Management System/Panel
- Bridge Navigational Watch Alarm System
- Electronic recorders/logs

Effects of human interventions

It should be possible to deselect the GNSS input to any NTP server via its settings menu, but in the worst case scenario the GNSS antenna input could be temporarily disconnected from the NTP server before entering a region of known GNSS interference.

Cargo Control

Onboard a modern vessel there could be a variety of cargo control systems that access GNSS data for position or time. These include environmental control systems, which may use time and position data to change temperature or thermostat levels, and shipment/container tracking systems which incorporate built-in GNSS trackers directly.

Mission Systems

Various systems such as dynamic positioning systems, surveying equipment, dredging processes, ROV/USV/AUV operations and many others can be entirely dependent on GNSS data. Anecdotal information from our survey has revealed that in some cases these secondary systems can be more resilient to GNSS interference than the navigation receivers used on the bridge, however, they are not approved by the IMO for the purpose of navigation. As before, a bespoke audit/connectivity diagram of all of the systems connected to GNSS for position or time is recommended to ensure a thorough understanding of the potential impact on any vessel activities that can be caused by GNSS interference.

5

Guidance for operating within GNSS interference regions

This section provides guidance for mariners, operators and owners on how to prepare before, act during, and recover from transiting GNSS interference regions. These recommendations assume that a vessel is ocean going (GMDSS sea area A3/A4) and therefore has to meet those SOLAS requirements. However, these recommendations are also considered 'best practice' for all vessels, no matter how close to shore they operate. A later section of this report (Section 6) deals with potential solutions to GNSS interference that involve installing resilient equipment or services, whereas the information here provides actionable steps that can be carried out for any vessel today. This section also provides simple, one-page guidance documents/checklists, each tailored for slightly different audiences: the vessel owner/manager/operator, the vessel master/navigator and the vessel officer of the watch. These are intended to be used as templates and adapted/tailored by the reader as appropriate for their vessel, operations, and crew. The guidance assumes that the GNSS connectivity diagram (see Section 4) has been created for the vessel and is a reference that can be used during the below procedures.

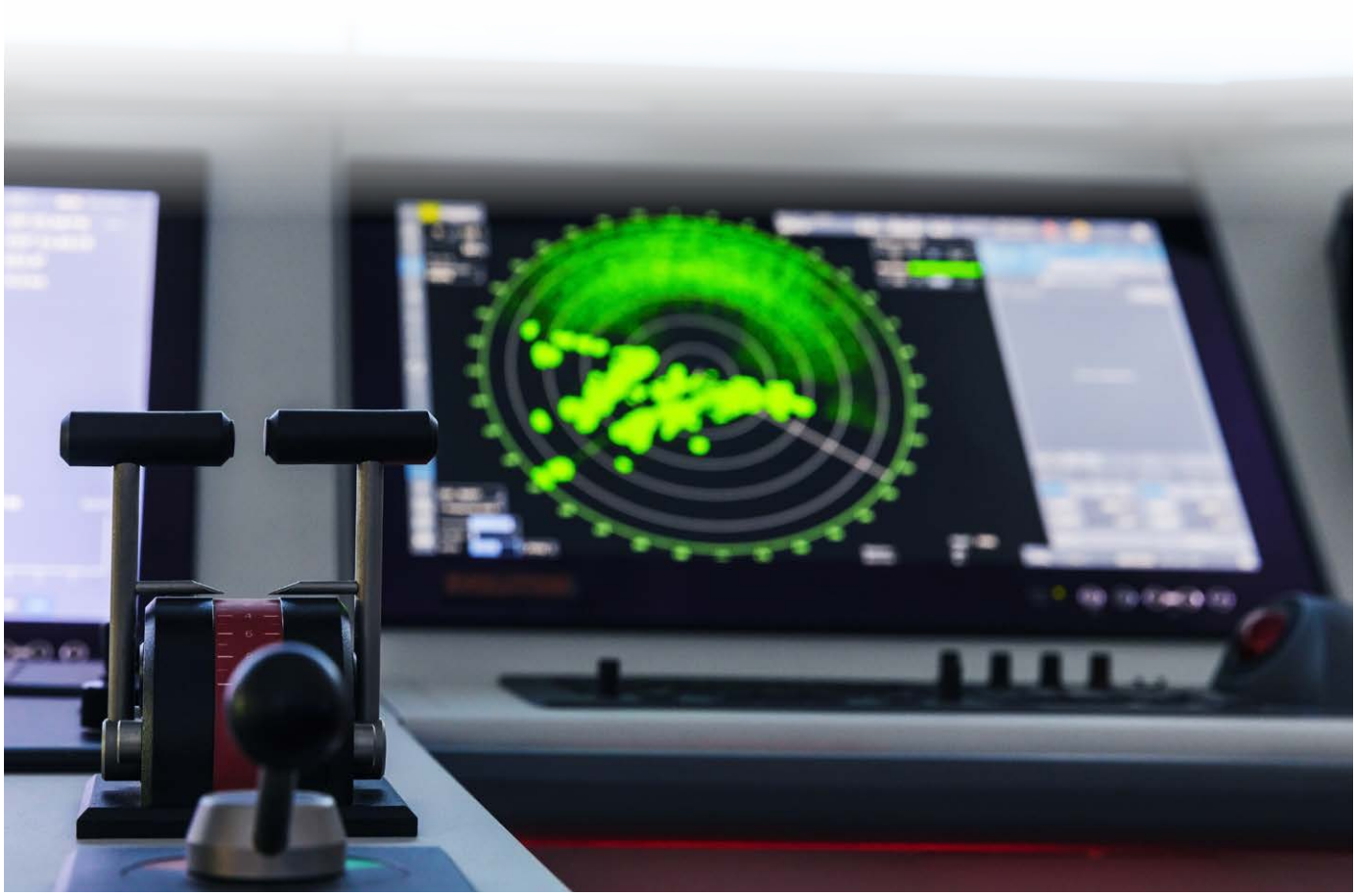
This section also provides simple, one-page guidance documents/checklists, each tailored for slightly different audiences.

In general, an abundance of caution is required before entering GNSS interference regions. If GNSS spoofing occurs, then the spoofed GNSS receiver will pass incorrect position, velocity and time to all of the systems listed on the vessel's GNSS connectivity diagram. This can occur in the first few milliseconds of GNSS spoofing, and so manually disabling systems only after signs of spoofing are obvious to people on the bridge is too late. By this time, a significant amount of damage could have been done from a cybersecurity point of view. Passing incorrect time to digital systems can have lasting effects well beyond the period spent within the interference region for a wide range of reasons, including invalidating digital certificates, causing the unwanted deletion of data, and causing incorrect data to be stored in memory and processed some time later. While it may not be practical, it would be ideal to power off all vulnerable GNSS receivers before entering an interference region, and only power them up again once the GNSS interference has confidently ceased. With this in mind, disabling access to GNSS data feeds from vulnerable receivers as much as possible before entering an interference region is strongly recommended.

Spoofing attacks include the broadcasting of incorrect data to the victim GNSS receivers. To be confident that no incorrect data remains stored in the memory of any digital system that has been exposed to spoofed GNSS data, power cycling equipment that has remained connected to GNSS data during a spoofing attack is the only way to guarantee "flushing out" any residual corrupted information. Again, while this may not be practical, it is unfortunately the only way to ensure that equipment will work as designed after being exposed to a GNSS-spoofing cyber attack. **It is important that all GNSS receivers are fully power cycled, or forced to "cold reset/cold**

reacquire", after leaving a spoofing region. This is because it is possible for GNSS receivers to appear to have recovered on their own (i.e. output valid position, velocity and time) after the vessel leaves an interference region, but sometime later the GNSS receiver could access corrupted data stored in its memory from the spoofing encounter, and only then output incorrect position, velocity and time. A detailed explanation of this issue is provided in the OpsGroup report into GPS spoofing on pages 33-35[21]. In our survey, around 5% of the respondents reported experiencing issues with their GNSS receivers sometime after leaving the interference regions.

Good guidance on the use of electronic navigation aids exist, such as MGN 37[22] and it is assumed here that these standard procedures are also being followed.



[21] https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf
[22] https://www.gov.uk/government/publications/mgn-379-mf-amendment-1-use-of-electronic-navigational-aids

GNSS INTERFERENCE GUIDANCE – OWNER / MANAGER / OPERATOR

PREPARE (BEFORE VESSELS DEPART FOR INTERFERENCE REGIONS)

Policy

- ☐ Review ISM Policy, including GNSS denial/spoofing as part of cyber security threat
- ☐ Ensure the company understands the risks. Complete the RIN checklist for GNSS vulnerability[23]
- ☐ Review the platform recovery plan and the interdependencies on the vessel GNSS Connectivity Map
- ☐ Monitor geographical areas of risk against the planned route of the vessel. Prepare to aid rescue services with detailed journey information if an incident occurs while the vessel is undergoing GNSS interference
- ☐ Put warning processes in place to inform vessels of any changes
- ☐ Define procedures to be followed by the master/bridge team should the vessel experience an event, including recovery procedures
- ☐ Establish the reporting policy for vessels, if they consider that a GNSS attack is occurring
- ☐ Identify responsibilities for all involved at HQ and onboard

Equipment/Systems

- ☐ List equipment reliant on GNSS for PNT, and their options for backup sources. Note any interference protection measures/equipment
- ☐ Provide recovery plans for each vessel in the fleet, especially considering differences between vessels of the same class. Ensure GNSS-independent navigation equipment is available

Training

- ☐ Provide cyber threat training for all personnel
- ☐ Practice the team response to the GNSS interference threats including the use of traditional navigation methods
- ☐ Ensure that Company-mandated ECDIS / ECS training for all bridge watchkeepers includes type-specific training identifying and countering GNSS denial/attack/spoofing
- ☐ Ensure training for all departments onboard includes actions for countering GNSS denial/spoofing on their equipment/systems (machinery/propulsion/habitability/SOLAS equipment/communications and IT)

ACT (VESSELS CURRENTLY WITHIN GNSS INTERFERENCE REGIONS)

- ☐ Acknowledge reports from ships affected and promulgate to appropriate, responsible organisations:
- ☐ USCG/UKMTO/MDAT-GOG (All GNSS interference events to be reported to relevant bodies)
- ☐ Regional NAVWARN authority
- ☐ Coast Guard HQ or coastal state authority for the area (unless the vessel has already done so)
- ☐ Other ships in fleet in the vicinity or approaching the area
- ☐ Be ready to seek OEM guidance for subsequent actions and recovery

RECOVER (AFTER VESSELS HAVE LEFT GNSS INTERFERENCE REGIONS)

- ☐ Report region of interference and region of successful recovery of GNSS to notified authorities
- ☐ Await requests for OEM recovery support
- ☐ Continue warnings to vessels approaching the region affected, unless notified by a responsible authority, that all interference activity has ended

[23] https://rin.org.uk/mpage/Resilient_PNT_Checklist

GNSS INTERFERENCE GUIDANCE – MASTER / NAVIGATOR

PREPARE (PRE-DEPARTURE / BEFORE ENTERING GNSS INTERFERENCE)

Policy

- ☐ Ensure all personnel understand the ISM Policy for GNSS outages
- ☐ Check the latest GNSS interference reports and locations
- ☐ Assess the likely impact of GNSS interference on the voyage, particularly in relation to the passage plan and brief the watchkeepers
- ☐ Ensure all watchkeepers are aware of their responsibilities and who they should call in the event of GNSS interference (eg: on watch engineer, master, additional personnel)
- ☐ Nominate additional watchkeepers who can be called upon to support the bridge team, (follow procedures for fog-lookouts if restricted visibility was forecast)
- ☐ Know your ECDIS / ECS and RADAR capabilities and limitations, including the setting changes required to maintain functionality of these systems once in an area of GNSS interference
- ☐ List the priority fallback alternative PNT sources in order of use in the event of a failure
- ☐ Set the 'check fix' policy for each leg of the passage plan
- ☐ Ensure a Bridge Emergency Card is ready on the bridge (e.g. "What to do when encountering GNSS Interference")

Equipment/Systems

- ☐ Create a GNSS connectivity map and ascertain the likely impact of GNSS interference on the ship's systems including identification of critical and non-critical systems

Training

- ☐ Ensure all watchkeeping personnel are informed and suitably trained to adopt the above policies
- ☐ Practice for GNSS interference as part of the normal ship's training regime, including equipment settings
- ☐ Maintain traditional navigation practices and emphasise the importance of GNSS-independent operations

ACT (DURING GNSS INTERFERENCE)

- ☐ Monitor OOW actions and completion of checklist
- ☐ Consider aspects of vessel safety likely to be affected by the outage
- ☐ Report outage to appropriate authorities in accordance with company policy
- ☐ Review the passage plan for safety

RECOVER (AFTER LEAVING GNSS INTERFERENCE)

- ☐ Receive confirmation of the recovery of the primary position source or oversee as necessary
- ☐ Report recovery to Owner/Manager/Operator
- ☐ Report recovery to local CG or responsible Maritime authority for the area
- ☐ Establish list of equipment still suffering residual effects and seek OEM guidance through Owner/Manager/Operator
- ☐ Assess whether it is safe to continue passage as planned, or whether a slower speed and/or additional measures are required until well clear of the danger area

GNSS INTERFERENCE GUIDANCE – OFFICERS OF THE WATCH

PREPARE (PRE-DEPARTURE)

Policy

- [ ] Read the company ISM Policy for GNSS outages
- [ ] Know if and when GNSS interference is expected on your watch

Training

- [ ] Review the bridge check off lists for GNSS outages and practise the requirements, including:
- [ ] Practise changing the primary and secondary position sources in ECDIS / the ECS as well as changing it to fix DR/EP mode with appropriate fix intervals in accordance with the check fix procedure
- [ ] Rehearse the check fix procedure with multiple fixing methods
- [ ] Practise changing the RADAR settings if position, heading and/or SOG become unavailable (recommend use head up, sea stabilised and STW)

ACT (DURING GNSS INTERFERENCE)

- [ ] Interrogate alarms and monitor equipment to determine if the vessel is being subject to GNSS interference
- [ ] RADAR image overlay (RIO) offset
- [ ] GNSS position / time unavailable or clearly incorrect compared to alternative independent sources
- [ ] Conduct immediate check fix to determine if the vessel is in safe water and change the ECDIS / ECS to fix DR/EP mode or approved alternative positioning source in accordance with the check fix procedure
- [ ] Report GNSS interference to the master and on-call engineer
- [ ] Call additional watchkeepers to the bridge as necessary and consider safe speed
- [ ] Use all available means to navigate and determine the position of the vessel, in addition to the check fix procedure (including the use of parallel indices on the RADAR and depth verification via the echosounder)
- [ ] Cross check alarm indications against the GNSS connectivity diagram for your vessel
- [ ] Assess other equipment on the bridge for signs of interference, using the vessels' connectivity diagram for reference, and report any impacts to the master and on-call engineer
- [ ] Request the master's approval to issue a warning to the local authority / coast guard / VTS or other vessels in the vicinity
- [ ] Monitor RADAR to correlate tracks for collision avoidance, especially in restricted waters and poor visibility
- [ ] Do not rely on AIS for collision avoidance or as a source of position/time
- [ ] Do not expect your equipment to respond in the same way every time GNSS interference is experienced

RECOVER (AFTER LEAVING GNSS INTERFERENCE)

- [ ] Continue check fix procedure
- [ ] Fully reset the GNSS receiver (e.g. power off and on again) to ensure all spoofing data is wiped from memory and determine if GNSS has become, and remains, accurate
- [ ] Request master's approval to return to GNSS as the primary position source in ECDIS / the ECS
- [ ] Continue to monitor RADAR to correlate tracks and identify if GNSS denial/spoofing is still affecting other vessels in the vicinity
- [ ] Monitor NAVWARNS and GMDSS messaging for further reports of activity
- [ ] Continue to monitor all equipment to determine if there are any residual effects of interference impacting any of the ship's systems and report as necessary
- [ ] Stand down additional watchkeepers and ensure the incident is accurately recorded in the ship's logbook

6 Solutions

This section contains information on various solutions that can reduce the impacts of the issues discussed in this report due to GNSS interference. These solutions are wide ranging, including enhancements to GNSS receivers themselves, alternative PVT solutions, and future technologies. The section concludes with some clear recommendations.

There are a wide range of existing maritime positioning and navigation techniques and technologies such as RADAR position fixing, echosounder depth transects, horizontal sextant angle, celestial fixes, and so on. It is assumed that the reader is well versed in these traditional systems and their strengths and weaknesses. This section will focus on providing an overview of the current and future solutions that may not be as well known to the mariner.

Hardened GNSS Solutions

To improve the robustness of GNSS against interference, various hardening techniques can be employed, such as signal authentication, encryption, anti-jamming and anti-spoofing measures. Implementing these measures can help to prevent spoofing and jamming attacks, and ensure the continued availability and accuracy of GNSS signals.

Multi-GNSS and Multi-Frequency

Legacy GNSS receivers (e.g. systems dating from 2015 or earlier) in use in Maritime may be single frequency, and single constellation, for example using only the USA GPS signals within the L1 frequency band. Modern receivers are capable of using multiple GNSS constellations and multiple frequency bands. It is possible that in some interference regions the jamming and spoofing signals may only be affecting a subset of these constellations and frequencies. It may therefore seem attractive to assume that if receivers are capable of using different constellations and frequencies then this may provide some form of protection against the interference. However **this is not a recommended solution to the problem of GNSS interference** for the following reasons:

1. There is no technical barrier to jamming all of the GNSS frequency bands, especially using sweep-jamming systems where jamming multiple frequency bands does not impact jamming range. There is also plenty of evidence in the public domain that all of the GNSS frequencies are suffering interference. (e.g. see reports from monitoring systems such as CGI SignalSense[24] and also the 2025 report from GPSPatron[25]).

2. Similarly, the barrier to entry for spoofing more than one constellation is also much lower in 2026 than it was 5-10 years ago. There are multiple open-source software repositories freely available on the internet that can simulate multi-constellation and multi-frequency broadcasts (for example https://github.com/globsky/SignalSim).

3. Meaconing is a type of interference where real data is recorded in one location, and then replayed at a different location and time (sometimes it is simply rebroadcast immediately). The cost and complexity of "record and replay" devices is very low indeed. Recording and rebroadcasting data from the L1, L2 and L5 bands at high power is not technically challenging.

4. Simply being **capable** of using open signals from multiple frequencies and multiple constellations does not in any way provide any inherent anti-spoofing capabilities at all. Specific anti-spoofing algorithms need to be deployed on the receivers, and these are in general proprietary, manufacturer, model, and firmware specific. Most non-military receivers designed and sold before 2020 that are capable of using 4 GNSS constellations and more than one frequency will still function and output data even if they are only detecting a single frequency and a single constellation, even though this is a clear indication of spoofing. Most legacy non-military receivers were designed before the current era of widespread GNSS jamming and spoofing and therefore lack anti-spoofing features. This is clearly evidenced from the first Norwegian Jammertest trials conducted in 2022[26]. A universally-acknowledged outcome of that trialling was the realisation that the majority of consumer GNSS receivers at that time were trivially jammed and spoofed in most attacks. Quoting from the report *"An unfortunate observation was that some high-end receiver systems supporting quadruple constellation triple frequency operation could be driven into apparently unrecoverable states via the single-frequency spoofing and multi-frequency jamming combinations of even the simple spoofing tests. Despite having an internal oscillator that is relatively stable, the receiver transitioned from tracking real signals to tracking the spoofed signals after only a short period of jamming but then would not recover after the removal of the spoofing and jamming."* One participant in the trials allowed their multi-constellation-capable smartphone to run the Strava app during one of the spoofing trials, and so posted their "personal best" to the Strava website of a 6.4km run in less than 6 minutes.

*Simply being **capable** of using open signals from multiple frequencies and multiple constellations does not in any way provide any inherent anti-spoofing capabilities at all.*

[24] https://www.linkedin.com/posts/stephen-vance-b4ba1111_tankers-collide-in-strait-of-hormuz-activity-7396860421040742400-AH2-/
[25] https://gpspatron.com/new-gnss-interference-report-released-shipborne-measurements-near-the-kaliningrad-border/
[26] Morrison, A., Sokolova, N., Solberg, A., Gerrard, N., Rødningsby, A., Hauglin, H., Rødningen, T., & Dahlø, T. (2023). Jammertest 2022: Jamming and Spoofing Lessons Learned. Engineering Proceedings, 54(1), 22. https://doi.org/10.3390/ENC2023-15445

Recommendations

When selecting new multi-constellation and multi-frequency GNSS receivers it is recommended that the manufacturer is asked to demonstrate the performance of the system when undergoing a bank of jamming and spoofing tests (e.g. ask to see specific results from the annual Norwegian JammerTest[27] event).

Dual Antennas

Dual-antenna GNSS receivers typically use the two antennas to provide an accurate estimate of the heading of the platform that they are mounted to. They do this by performing a local carrier-phase positioning estimate to determine the orientation and length of the baseline at a sub-radian and sub-decimetre resolution. When such a system encounters spoofing, both antenna positions will be calculated to be at almost identical positions, and not actually to be separated by the known/expected baseline. Assuming that the dual antenna system is running software that will detect and and activate an alarm under this condition, it is possible for dual antenna systems to raise a spoofing alarm message and to cease outputting data until such time as the measurements make sense again (i.e. when the interference ceases). This therefore provides an effective spoofing detection (but not rejection) technique. More advanced signal processing, such as combining the data from two antennas in order to steer a null of insensitivity, is possible, and is described in the CRPA section below.

Recommendations

Dual antenna systems are capable of detecting spoofing attacks and ceasing to output data until the interference has ceased. They do not inherently provide any jamming protection.

Controlled Reception Pattern Antennas (CRPA)

The CRPA is a type of antenna that is specifically designed to protect against the effects of jamming and spoofing of GNSS signals. CRPA combines the signals received simultaneously across an array of multiple antenna elements in controllable ways that allow signals from specific directions to be attenuated and signals from other specific directions to be amplified. This allows the CRPA to prevent jamming, and in some CRPA designs spoofing signals too, from reaching the GNSS receiver. In advanced CRPA designs this

[27] https://jammertest.no/jammertest-2025/

can be performed while simultaneously amplifying the true signals arriving from each satellite. CRPA design and complexity varies significantly. In order to handle more interference sources simultaneously, more antenna elements are required, which increases size and computational demands.

CRPA are an attractive solution to Maritime GNSS interference because, in principle, they can be acquired as standalone systems that don't require changes to the GNSS equipment on the bridge itself. However, a significant issue as highlighted in this report, is that there are many systems on a modern vessel with a built-in GNSS receiver, such that not all GNSS data will be sourced through a single CRPA on the vessel. The CRPA antenna is generally larger than typical GPS antennas due to the multiple antenna elements and associated electronics that are required to achieve its functionality.[28] However for most maritime applications this is not expected to be an issue. The cost of CRPA is much higher than for standard antennas (e.g. thousands of US dollars rather than hundreds) but these prices are expected to reduce over time now that GNSS CRPA have been removed from the US ITAR (International Traffic in Arms Regulations) export control list[29].

Recommendations

CRPA are expensive and bulky antenna systems, but they provide the best option for defeating high-powered jamming. Some CRPA designs can also ignore spoofing attacks while maintaining true GNSS signal availability within interference regions. In any case, anti-jamming "only" CRPA antennas can greatly assist in preventing the receiver from falling back into "acquisition mode" where it is most vulnerable to a spoofing attack (i.e. most successful spoofing attacks rely first on jamming the receiver and forcing it back into acquisition mode). Type approvals and performance standards for maritime CRPA should be urgently established.

Advanced Signal Processing

There is extensive academic and commercial literature on receiver architectures and algorithms that can be used to provide robustness against jamming and spoofing. Simple tone-based jamming can be overcome with notch filters for example. Naive spoofing can be ignored by maintaining tight tolerances on navigation engine jumps in position or time that are physically impossible. The majority of consumer-grade receivers designed before 2020 have little to no spoofing protection built into them because such algorithms were simply not part of the original specification or feature list. Future receivers are likely to have much more extensive anti-spoofing capabilities.

[28] GPS World, Anti-jam technology: Demystifying the CRPA, April 12, 2017
[29] https://www.gpsworld.com/crpas-for-pnt-removed-from-itar-list/

Recommendations

When selecting new multi-constellation and multi-frequency GNSS receivers it is recommended that the manufacturer is asked to demonstrate the performance of the system when undergoing a bank of jamming and spoofing tests (e.g. results from the annual Norwegian JammerTest[30] event).

Galileo Open Signal Navigation Message Authentication (OSNMA)

OSNMA[31] was declared fully operational on 24th July 2025. The era of relying on open GNSS signals for safety-critical systems is finally over. OSNMA provides a cryptographic watermark overlaid on E1-B Galileo GNSS signals that allows a receiver to detect whether spoofing is currently taking place. The process of detecting spoofing takes a number of seconds to perform (due to the time taken to download the required watermarks from the signal itself) and future receiver designs, and future dependent systems, will need to take this timing lag into account. Care will need to be taken, especially with digital systems that use GNSS position and time data immediately wherever it is created, as to how they might handle the information that they have been processing spoofed data for a number of seconds by the time the alarm is raised. In practise this is not an issue as long as the OSNMA GNSS receiver is combined with an inertial navigation system and a stable oscillator (timing reference) to bridge the gaps in position, velocity and time between the authenticated epoch and the current epoch.

OSNMA[31] was declared fully operational on 24th July 2025. The era of relying on open GNSS signals for safety-critical systems is finally over.

Recommendations

The use of OSNMA and other authentication schemes is strongly recommended to provide anti-spoofing protections. Systems integrations must carefully design their systems to ensure that any delay-to-authentication issues are carefully managed as GNSS data is distributed to various other systems.

[30] https://jammertest.no/jammertest-2025/
[31] https://insidegnss.com/osnma-necessary-but-not-sufficient-for-gnss-security/

GNSS Signal Encryption

GNSS signal encryption is a technique used to protect GNSS signals from unauthorised access. This is done by encrypting the signal using a secret key. The encrypted signal can only be decrypted by an authorised receiver, and cannot be spoofed by an unauthorised transmitter. Some examples of GNSS encryption are the GPS P(Y) and M codes for military use, and the Galileo PRS. At this time there are no encrypted signals broadcast by GNSS satellites that are accessible to the civilian maritime sector. Future corporate offerings from LEO service providers may include encrypted signals.

Recommendations

A watching brief should be kept on the availability of encrypted signals from space for safety critical systems over the coming years.

Complementary and Alternative PNT

Complementary PNT refers to the use of non-GNSS positioning and timing technologies that can provide resilient and reliable navigation and timing solutions for maritime vessels. This list is not exhaustive, existing "standard" maritime navigation systems are not included as the authors assume the reader is well versed in their strengths and weaknesses already.

Inertial Navigation Systems

Inertial Navigation Systems (INS) can be used in maritime navigation to continuously estimate a vessel's position, velocity and heading by utilising real-time measurements of speed, direction, and rotation. These measurements are typically provided by an Inertial Measurement Unit (IMU) containing accelerometers and gyroscopes. In some cases magnetometers and pressure sensors are also incorporated. INS allows for the modern form of dead reckoning, where position updates are estimated over time based on an initial position fix being updated by regular speed and heading measurements or estimates. The accuracy of INS degrades over time due to noise and other error sources on the accelerometer and gyroscope measurements accumulating over time. INS are regularly updated by external estimates of position, velocity, and orientation, with GNSS being a standard source of these corrections.

Recommendations

An INS is an excellent addition to a modern vessel to provide navigation updates during short GNSS outages, noting that their accuracy degrades over time without corrections from external sources.

Visual and Lidar-based navigation

These technologies use cameras or Laser Imaging Detection & Ranging (lidar) to provide information on how a vessel is moving relative to its surroundings. These systems are more common in automotive and drone applications. In maritime the issues of sea spray and the criticality of good navigation aids in poor visibility limit their use in this sector.

Quantum inertial navigation

Quantum inertial navigation technology refers to new inertial measurement units that exploit fundamental quantum properties (entanglement and/or superposition)[32]. The aim of these new sensors will be to provide navigation-grade inertial measurement units at a lower price point or smaller size, weight and power than the existing navigation-grade solutions. This technology has the potential to improve the safety and efficiency of maritime operations, particularly in areas with limited or no GNSS coverage. However, the Technology Readiness Level of this technology is currently low, with the expectation to improve in the following years as research and development continue to advance. Quantum INS will also require very accurate and high resolution gravity maps (these are vital corrections for high performance INS) which are not currently available or maintained covering every location on the Earth.

[32] Quantum Sensors for Navigation – From Physics to Field Deployment https://www.youtube.com/watch?v=NMbM7IW5Fwg

eLoran

Enhanced LORAN (eLoran) is a long-range terrestrial radio navigation system designed to provide PNT without any reliance on GNSS. It is a modernisation of the traditional LORAN-C systems. Notably however the signal has been modernised as have aspects of the overall positioning system, such that there is no longer a concept of "Master" and "Slave" transmitters and instead eLoran uses an "all in view" ranging method like GNSS do. eLoran operates by utilising powerful (e.g. many tens of kiloWatts), low-frequency radio transmitters, broadcasting signals that are significantly stronger than satellite signals. The low frequency (100kHz) signals are also more difficult to jam and spoof at long distances than the UHF signals used by GNSS. The position and timing accuracy of eLoran is around an order of magnitude lower than for GNSS but for many maritime applications this is still acceptable. Performance can degrade further due to "skywave" interference when the signal reflects from the ionosphere and interferes with the usual "groundwave" signal that propagates over the surface of the Earth; however, this can be mitigated with modern signal processing techniques. Some nations including South Korea, Saudi Arabia, China and Russia maintain eLoran networks, and the UK has recently announced an intention to develop sovereign eLoran positioning capabilities on top of the existing timing system[33].

eLoran operates by utilising powerful (e.g. many tens of kiloWatts), low-frequency radio transmitters, broadcasting signals that are significantly stronger than satellite signals.

Ranging Mode

Ranging Mode (R-mode) is a proposed system that will utilise existing broadcast infrastructure to provide a cost-effective backup solution for Positioning, Navigation, and Timing information. Currently, it consists of two subsystems: VDES transmission in the VHF band, and the maritime DGNSS service in the MF band. The use of spread-spectrum techniques, combined with the high-power signals (compared to GNSS) allow for a high resilience against jamming attacks[34].

With the ongoing European ORMOBASS and ESA MAPS projects, R-Mode will be in a pre-operational state in 2026 within the Baltic.[35] Positioning accuracies of approximately 10 metres were achieved through testing the Ranging signal on the VDES communications signal in controlled environments[36]. R-Mode is also being tested in other regions worldwide, with notable testing taking place in South Korea and Canada. Limitations of the system include reduced accuracy during the night for the MF signal, due to changed propagation properties and the limited line of sight in the VDES signal.

[33] https://www.gov.uk/government/news/landmark-government-investment-to-safeguard-the-essential-signals-we-all-rely-on
[34] Grundhöfer, Lars (2024) R-Mode: An Alternative to Global Navigation Satellite Systems for Terrestrial Navigation at Medium Frequencies. DLR-Forschungsbericht. DLR-FB-2024-9. Dissertation. TU Ilmenau. 175 S. doi: 10.57676/dy71-6t71 <https://doi.org/10.57676/dy71-6t71>.
[35] https://interreg-baltic.eu/project/ormobass/
[36] M. Wirsing, A. Dammann and R. Raulefs, "Positioning Performance of VDES R-Mode," 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021, pp. 1-6, doi: 10.1109/VTC2021-Fall52928.2021.9625258. keywords: {Performance evaluation;Global navigation satellite system;Receivers;Estimation theory;Lakes;Distance measurement;Kalman filters},

Signals of Opportunity

Many signals that are primarily designed for communications can also be utilised for PNT applications. Terrestrial signals from cellular, Digital Audio Broadcasting (DAB) radio, or Digital Video Broadcasting Terrestrial (DVB-T) transmitters have been the source of much academic, and some industrial, activity in this space. In the last few years a lot of research has also gone into using LEO communications satellites as opportunistic PNT sources too. In the smartphone sector, opportunistic positioning using WiFI signal strength databases has been a reliable indoor positioning technique for over 20 years in use by Google, Apple and others, although these are less applicable in the maritime environment.

Low Earth Orbit (LEO) PNT systems

Low Earth Orbit constellations of satellites can provide global PNT signals. Traditional GNSS are further away in Medium Earth Orbits (MEO), and so the received signal power from a MEO satellite is much lower than for a LEO satellite with the same transmit power. Dedicated PNT service providers such as TrustPoint and Xona Space are still expanding their capabilities and constellation size. Communications systems providers such as OneWeb and Starlink may choose in future to provide dedicated PNT signals, or there may be "unsupported" PNT provision from these communications constellations using opportunistic radio positioning receivers as mentioned above. Due to limited frequency choice and limited transmission power, it remains open how effective these systems are against jamming attacks[37]. To counter spoofing it is likely that commercial LEO PNT service providers will offer encrypted signals to their customers.

[37] https://insidegnss.com/leo-pnt-a-fundamental-evolution-to-answer-new-application-needs/

Summary

There is no clear "golden bullet" to solving the problem of GNSS interference in the maritime sector, but a number of recommendations can be made:

- The most effective change that can be made to mitigate the issues of long-range GNSS jamming is to install anti-jamming Controlled Reception Pattern Antennas (CRPA). Preventing jamming can also prevent some spoofing attacks (as discussed in Section 2).
- Care must be taken when considering the potential impact of multi-frequency and multi-constellation receivers. These capabilities alone give no protection against multi-frequency jamming and multi-constellation spoofing, both of which are trivial in 2026, and are known to be prevalent according to recent studies of the major interference regions[38].
- Safety-critical systems should not rely on open (spoofable) signals in the future, as we do today. Authentication schemes, such as Galileo OSNMA, provide a level of spoofing detection. Extensive anti-spoofing signal-processing and sensor-fusion techniques exist, and procurement teams within the maritime sector should ensure that GNSS receivers being advertised to them can withstand a bank of industry-approved GNSS interference tests, such as those deployed at the annual Norwegian JammerTests[39].
- Current and future non-GNSS space-based signals from satellite communications companies and from dedicated PNT providers should be considered, especially those offering authentication and encryption capabilities.
- Vessels operating in waters where high-power terrestrial signals (e.g. eLoran, R-Mode) are currently available, or are planned, should consider adding the necessary receivers to make use of these high-powered alternatives to GNSS.
- The number of systems on a modern bridge that are unnecessarily connected to GNSS data sources should be reduced. Timing references and Master Clocks that are independent of GNSS should be preferred by any vessel expecting to traverse GNSS interference regions.

[38] https://www.linkedin.com/posts/stephen-v-b4ba1111_tankers-collide-in-strait-of-hormuz-activity-7396860421040742400-JwBc
[39] https://jammertest.no/

Summary and Recommendations

This report has highlighted a number of urgent concerns:

- A modern digital vessel uses GNSS position and time data for a variety of navigation and non-navigation purposes. During GNSS spoofing, dozens of devices onboard a modern vessel can therefore process incorrect time and/or position, and can display or store incorrect information. This is a significant cyber security issue, and the assessment and management of the issues must be considered within cybersecurity frameworks.
- Global Maritime Distress and Safety Systems (GMDSS) and International Convention for the Safety of Life at Sea (SOLAS) mandated equipment that use GNSS as their primary source of position and time are highly vulnerable to GNSS interference and these systems may report incorrect time and position if used during distress when within GNSS interference regions. This list includes GMDSS, EPIRB (Emergency Position Indicating Radio Beacon), AIS-SART, and MOB (Man Over Board) quick-push buttons.
- Vessels are currently being chartered through known GNSS interference regions when it is known that their GMDSS and SOLAS equipment will not function correctly in those regions. This raises significant concerns around liability and the responsibility for the safety of the vessel, including the potential for harm to personnel, property and the environment in the event of an incident directly attributable to GNSS interference.

Vessels are currently being chartered through known GNSS interference regions when it is known that their GMDSS and SOLAS equipment will not function correctly in those regions.

The survey results highlighted:

- The problems associated with GNSS interference have been getting worse.
- Manual interventions, including turning systems off and on again, are sometimes required to restore normal functionality to various systems after experiencing GNSS interference.
- Operating within interference regions significantly impacts workload, and often requires additional personnel to be assigned to the bridge.
- GNSS interference can result in vessels being put into unsafe or unlawful situations 14% of the time (1 in every 7 vessels).
- Damage to vessels, injury to personnel and environmental harm were all reported.
- Almost half of the respondents stated that GNSS interference has reduced their trust in their vessel and its systems.

The report's key recommendations include:

- Urgent addressing of the vulnerability to GNSS spoofing of SOLAS mandated systems, including GMDSS, EPIRB, AIS-SART, MOB quick-push buttons.
- Updating NAVWARNS broadcasts to include GNSS interference information.
- Establishment of a real-time global GNSS interference monitoring and mapping capability (similar to https://gpsjam.org/) with specific maritime focus[40].
- Industry-wide adoption of anti-spoofing improvements to GNSS receiver designs, especially when used in safety critical applications.
- The removal of unnecessary connections to open GNSS signals by hardware manufacturers targeting the maritime sector.
- Thorough testing of existing safety systems that incorporate GNSS within both jamming and spoofing test scenarios to confirm how they behave. If they do not behave as required, the manufacturers must urgently provide replacement systems or software updates.
- When selecting new multi-constellation and multi-frequency GNSS receivers it is recommended that the purchaser requests a demonstration of the performance of the receiver when undergoing a bank of jamming and spoofing tests (e.g. ask to see specific results from the annual Norwegian JammerTest[41] event).
- Installing antenna systems with anti jamming and anti spoofing features, such as CRPA.
- The use of OSNMA and other authentication schemes by GNSS receiver manufacturers is strongly recommended. Systems integrators must carefully design their systems to ensure that any delay-to-authentication issues are carefully managed as GNSS data is distributed to various other systems.
- The deployment and adoption of long-range terrestrial PNT systems such as eLoran and R-Mode is encouraged.
- Future SOLAS systems should not rely on open (spoofable) GNSS signals.

Based on the comprehensive analysis of the threats, impacts, and potential solutions related to GNSS interference, the workgroup issues the following specific recommendations to key stakeholders across the maritime industry.

[40] All existing websites use ADS-B data to derive interference regions, but the aviation sector has a much bigger radio horizon than maritime due to the significant altitude differences. Maritime interference regions
[41] https://jammertest.no/jammertest-2025/

For Masters, Navigators and Officers of the Watch

1. **Maintain an accurate GNSS connectivity diagram:** Assist the vessel owner / operator / manager in the creation of an accurate GNSS connectivity diagram, with the assistance of the engineers and equipment providers. Once complete, this should be maintained and updated onboard and regularly reviewed to ensure a thorough understanding of how the ship may be impacted by GNSS interference.

2. **Understand and follow the vessel's cyber-security policy:** Appropriate policies must be read, understood and followed as part of the vessel's safety management system (SMS).

3. **Understand onboard equipment:** It is vital that the vulnerabilities, limitations and alternative modes of operation of all onboard equipment and systems are thoroughly understood. Affected GNSS equipment must be power-cycled (switched off and on again) to ensure malicious data is cleared from memory after spoofing has occurred.

4. **Maintain awareness of where GNSS interference may be encountered:** Knowledge of the GNSS interference regions will allow for the adequate preparation of a suitable passage plan, equipment and personnel in both readiness for a jamming or spoofing attack and the ability to fully recover all systems once the attack has ceased or the vessel has left the region of GNSS interference. (See the checklists for PREPARE - ACT - RECOVER in Section 5 of this report.)

5. **Experience, knowledge and training:** Shared knowledge and experience will help to educate the onboard team and must be supplemented by regular training. Practising for encountering areas of GNSS interference should be treated as critical as any other emergency operation. Regular use of traditional navigation techniques will ensure these practices do not become a novelty, due to skill-fade, but instead remain important elements of the watchkeeper's toolkit.

6. **Report. Report. Report:** In order to maintain an understanding of the scale and impact of GNSS interference, it is vital that instances of jamming and spoofing are reported to the appropriate authorities. Additionally, the effect on equipment and ship's systems should be carefully monitored and reported to the owner/operator/manager and the relevant equipment providers.

For Vessel Owners, Operators and Managers

7. **Provision of a robust cyber-security policy:** The IMO and ISM (International Safety Management) Code provide guidance on the appropriate elements of cyber risk management[42]. This policy should be made available to the ship as part of their safety management system (SMS).

8. **GNSS vulnerability mapping:** An accurate GNSS connectivity diagram for each vessel should be created and maintained as part of the existing risk-register process. This should be used to provide guidance for the crews and to give them a checklist when encountering GNSS interference to ensure that all systems that may have been affected can be checked and verified to be working properly after the interference has passed. This is especially important for safety equipment.

9. **Provision of appropriate safety equipment:** No vessel should enter into GNSS interference regions without appropriate functioning safety equipment. For vessels where GNSS vulnerabilities are known to degrade the behaviour of the safety equipment currently in use, suitable replacements or augmentations should be made available before vessels embark to transit known interference regions.

10. **Provide adequate training:** Suitable training for how mariners should prepare for, act during, and recover their systems after encountering GNSS interference should be created and made available to crews.

11. **Invest in resilient PNT:** Develop a long-term strategy for upgrading vessel navigation suites to be more robust against GNSS interference. For vessels operating frequently in high-risk areas, conduct a cost-benefit analysis for retrofitting Controlled Reception Pattern Antennas (CRPA). Maintain technology roadmaps that monitor the availability of future robust PNT systems and upgrade GNSS hardware to receivers that incorporate specific anti-spoofing algorithms and authentication schemes such as OSNMA. When selecting new multi-constellation and multi-frequency GNSS receivers it is recommended that the purchaser requests a demonstration of the performance of the receiver when undergoing a bank of jamming and spoofing tests (e.g. ask to see specific results from the annual Norwegian JammerTest[43] event).

[42] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf
[43] https://jammertest.no/jammertest-2025/

For Maritime Regulators (IMO, Flag States, Governments)

12. **Establish resilience standards:** The International Maritime Organization (IMO), in coordination with flag states, should develop and mandate new performance standards for maritime PNT equipment. These standards should address robustness against GNSS & AIS jamming and spoofing, and should specify the bank of interference tests that a receiver is expected to pass before being suitable for use in safety-critical applications in the maritime sector.

13. **Enforce compliance** with flag state requirements when vessels operate with degraded systems.

14. **Establish live GNSS interference maps:** Establish a maritime-centric GNSS and AIS interference monitoring service that provides live maps of regions experiencing GNSS jamming and spoofing, and AIS spoofing, using data from monitoring stations and satcomms providers. Promote the use of these maps for planning routes and for warning mariners when they are approaching, transiting and leaving areas of GNSS interference. Such maps also provide an evidence layer that helps define regulation, deliver assurance, understand liability, and to enable informed investment decisions.

15. **Update NAVWARNS broadcasts to include GNSS interference information:** A modern weather report should include the current conditions for electronic interference in a given region. NAVAREA Coordinators to use the World-Wide Navigational Warning Service to issue Navigational Warnings on the subject of GNSS interference in their areas. Navigational Warnings are issued in response to SOLAS V/4 and carry information which may have a direct bearing on the safety of life at sea. This report will continue to highlight the impact of GNSS interference on safety of life at sea and deems this interference to meet the criteria for “new navigational hazards and failures of important aids to navigation” as well as “significant malfunctioning of radionavigation services and shore-based MSI radio or satellite services”, as determined by the Joint IMO / IHO / WMO Manual on Maritime Safety Information. Where possible, the issued NAVWARN should include the boundaries of the interference region and the duration, where known. This broadcast message could also include reporting options for affected vessels beyond the known boundaries of interference and where local authorities are collecting such data.

16. **Support eLoran and R-Mode infrastructure:** National governments and international bodies should actively support and fund the development and deployment of eLoran and R-Mode to supplement GNSS as resilient, dissimilar, and interoperable terrestrial PNT backup systems.

17. **Formalise incident reporting:** Establish a formal, global, and standardised mechanism, preferably under the purview of the IMO, for the reporting and dissemination of maritime GNSS interference events. This will provide authorities and the industry with a clear, real-time picture of the global threat landscape.

For Port Authorities and VTS Operators

18. **Implement local GNSS monitoring:** Install GNSS quality monitoring systems within port limits and critical approaches. These systems can provide early warning of interference events to both VTS operators and transiting vessels, and can contribute to global live GNSS interference monitoring maps.

19. **Develop VTS contingency plans:** Create and regularly drill contingency plans for managing vessel traffic during periods of widespread GNSS and AIS interference. These plans should emphasise procedures for navigation using RADAR, voice reporting, and other non-GNSS dependent methods.

For Equipment Manufacturers

20. **Improve GNSS receiver designs:** GNSS receivers for use in safety critical applications must improve their robustness to intentional jamming and spoofing. Incorporate anti-spoofing algorithms as standard, and incorporate authentication schemes such as Galileo OSNMA. Maintain technology roadmaps that monitor the availability of future secure radio navigation signals that incorporate authentication or encryption.

21. **Remove unnecessary GNSS connections:** The integration of GNSS receivers within maritime equipment should be carefully considered. Equipment containing GNSS receivers should include clear guidance on how the internal GNSS receiver can be isolated/disabled if required by the user.

22. **Improve interference testing:** All systems containing GNSS receivers should undergo aggressive jamming and spoofing trialling (e.g. as conducted at the annual Norwegian Jammertest trials) to determine and improve the level of vulnerability to different interference attacks. This is critical for SOLAS equipment.

23. **Update ECDIS software** to provide a "GNSS interference region mode" to quickly and easily change all required settings

24. **SOLAS equipment** must not depend on open (spoofable) GNSS signals for their safety-of-life functionality.

Appendices

Appendix A - AIS Interference

Uses of AIS

The Automatic Identification System (AIS) data was initially designed as a short-range collision avoidance tool for ship-to-ship and ship-to-shore communication, but it is now used for a variety of purposes including monitoring vessels for illicit and unsanctioned activities.

AIS acts as a low cost and low power situational awareness tool by broadcasting GNSS data over a communications link to allow vessels to easily share their position, velocity, identity and other useful data. This allows a "RADAR-like" view of the vessels within a given region without requiring RADAR systems.

Since AIS broadcasts can be detected by both land-based monitoring stations and from satellites, a global picture of all shipping in progress can be monitored continuously. In recent years, a secondary use of AIS data has been for regulators, financial institutions, insurers, and commodity traders to harness this data to perform due diligence and to enforce sanctions. It is an effective way to verify that a vessel is not calling at engaging in sanctioned trade, carrying out illicit ship-to-ship transfers or practising illegal fishing.

Manipulating AIS data

The reliability of this critical data source has been heavily impacted by the ease of access to AIS spoofing equipment and GNSS spoofing equipment. Both AIS and GNSS are open signal structures, and with the exception of the brand new Galileo OSNMA signal, they have no inherent authentication or encryption capabilities. This means that it is relatively straightforward to broadcast fake AIS or GNSS data, and therefore pretend that vessels are in different places than they really are.

Before third-party GNSS jamming and spoofing was common, any manipulation of AIS data was a strong indicator that the operators of the vessel were intentionally faking their broadcasts, known as first-party spoofing. However since third-party GNSS spoofing can also cause AIS data to be incorrect, it is now possible for bad actors to take advantage of or initiate GNSS interference in specific regions to disguise their malicious activities where possible, for example to perform ship-to-ship transfers, knowing that they would be "camouflaged" among the dozens or hundreds of other nearby vessels all also being spoofed to incorrect locations.

Regulators and other investigators can now however rely on high resolution satellite and SAR imagery to confirm the true locations of vessels regardless of their AIS broadcasts[44].

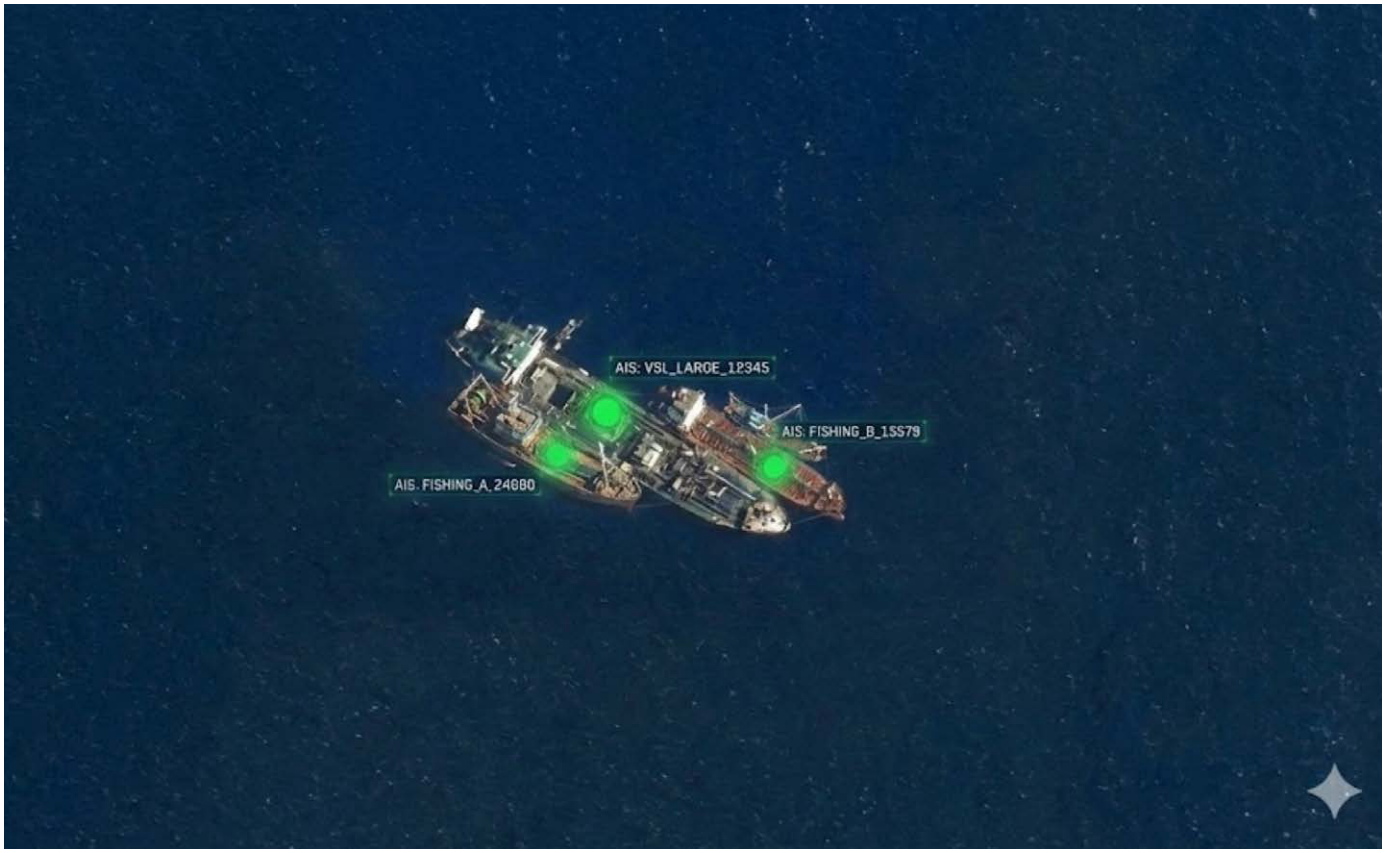


Figure A.1 is a mockup image of an illegal ship-to-ship transfer being captured on both satellite imagery and via AIS. Processing AIS data directly makes such detections trivial, as simple closest-distance calculations can be processed trivially in software across all AIS data. Without the AIS data, performing image analyses to determine whether ships are co-located is a much more complicated task, and also relies on good visibility (i.e. not under cloud cover or at night). In recent years however the availability of Synthetic Aperture RADAR imagery has enabled all-weather and 24-hour surveillance.

[44] https://www.bbc.co.uk/news/articles/cy8jvll9j81o

Impacts of AIS data manipulation

AIS data manipulation creates a number of issues:

- **Sanctions challenges:** AIS manipulation due to GNSS interference has led to more conflicts in due diligence and compliance checks because of the number of "innocent" vessels being impacted in high risk areas. According to Lloyds List Intelligence, there have been situations where vessels engaged in "clean" trade have been accused or questioned over potential sanctions violations, with owners and operators having to provide evidence to prove their data was tampered with. A prominent example involves tankers physically berthed in the Polish ports of Gdynia or Gdansk having their AIS broadcasts spoofed to appear as if they are located in completely different territorial waters. This would generate a red flag for compliance officers reviewing the ship's movements, requiring additional information, such as satellite imagery, to prove the vessel's true movements.
- **Convenient excuses:** The widespread nature of GNSS interference now provides a convenient cover for illicit actors. A captain caught with gaps in their AIS history or strange positional jumps can now plausibly claim that the issues were caused by third party GNSS spoofing, and not by their own manipulation of their AIS broadcasts.
- **Shadow fleet camouflage:** Similarly, if *all* ships in a particular region look like they are jumping around erratically, the one ship actually violating sanctions becomes impossible to isolate as its true behaviours are hidden.

Solutions to AIS manipulation

There are a number of issues that have led to these vulnerabilities:

- AIS messages are unauthenticated and unencrypted, and are relatively simple. AIS spoofing hardware is therefore cheap and easy to make. Modern Software Defined Radios compound this issue event further.
- GNSS spoofing leads directly to AIS spoofing, because the AIS system is designed to just rebroadcast GNSS data over a simple radio link.

Solutions to the AIS manipulation issues include:

- Expediting AIS authentication schemes. One such scheme is recommended by the UK GLA and IALA, and is fully backwards compatible. This scheme uses the VDES VHF communication link to broadcast a digital signature along with a corresponding AIS squitter[45].
- Feeding AIS transceivers with GNSS receivers that are robust to jamming and spoofing. This can be achieved in part by fitting a CRPA as discussed earlier in this report. In the near future, ensuring AIS transceivers are paired with OSNMA-compatible anti-spoofing GNSS receivers will also help.
- Feeding AIS transceivers with non-GNSS-based PNT data such as eLoran, INS data, or future secure LEO-based PNT signals. This is not trivial because AIS has been designed specifically to work entirely from GNSS data, and AIS systems often incorporate an internal GNSS receiver rather than using an external feed from elsewhere on the vessel.
- Easier access to low cost global high resolution imagery or SAR data for regulators and other key bodies to directly observe the locations and movements of vessels.
- Distributed multilateration techniques to allow distributed AIS receivers to geolocate each AIS squitter in order to cross-check the geolocated position estimate with the embedded GNSS data in the AIS data packets.

[45] https://academy.iala.int/e-bulletin/authenticating-ais-and-vdes-keeping-them-safe-for-another-generation-of-mariners/

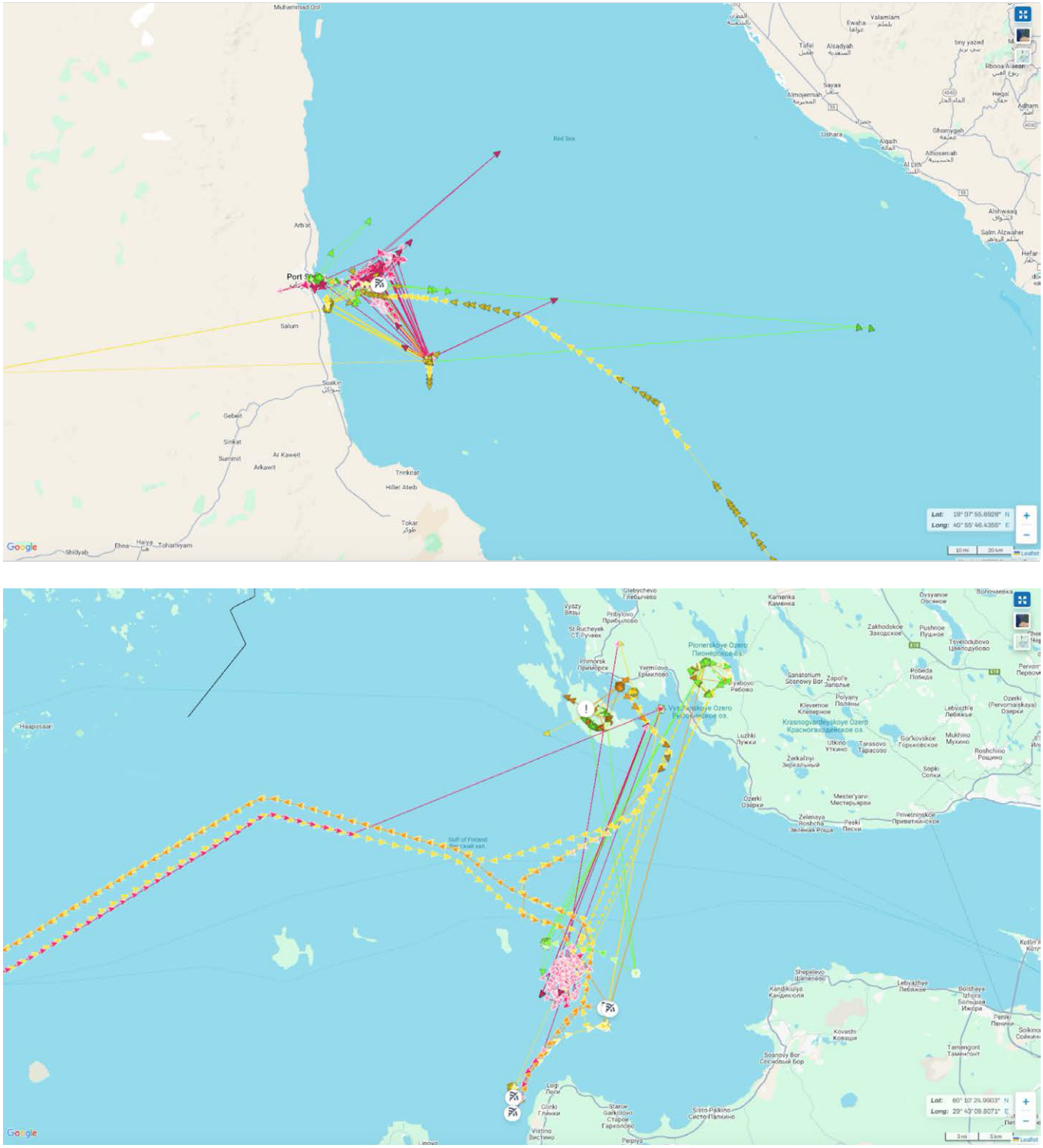


Figure A.2 shows the impact of GNSS interference and jamming on commercial vessels loading at Baltic ports (March 2025). Source: Lloyd's List Intelligence, Seasearcher.

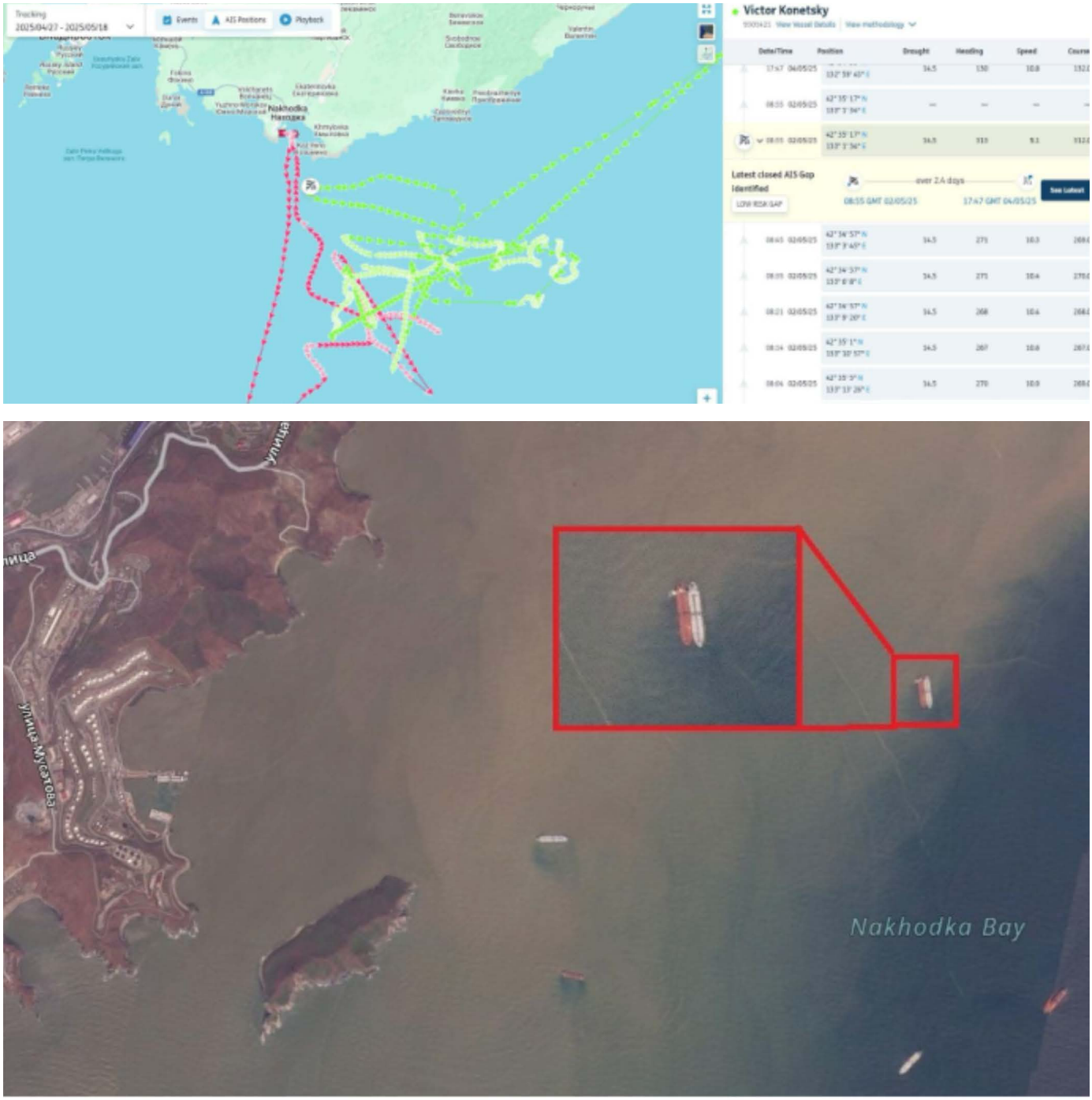


Figure A.3 shows the impact of GNSS interference and jamming on commercial vessels loading at Baltic ports (March 2025). Source: Lloyd's List Intelligence, Seasearcher. First-party spoofing was deployed so one tanker could load oil from a US sanctioned tanker, all while seemingly berthed at a distant port. Third-party spoofing, while less severe and consistent in this area, would mean that it is possible that in other instances this type of sanctions circumvention could play out without the requirement of third-party spoofing, as the background interference would effectively disguise this activity. The upper pane is an image from Lloyd's List Intelligence[46], Seasearcher. The lower pane is an image from Planet Labs PBC with mark-up by Lloyd's List Intelligence.

[46] https://www.lloydslist.com/LL1154016/Nakhodka-Bay-becomes-new-STS-hub-for-sanctions-skirting-tankers

Appendix B - VTS and GNSS Interference

Authors: Thomas Southall (IALA) & Kevin Gregory (Trinity House)

VTS and GNSS Interference

Introduction

A Vessel Traffic Service (VTS) has the capability to interact with traffic and respond to developing situations within a VTS area to improve the safety and efficiency of navigation, contribute to the safety of life at sea and support the protection of the environment.

To fulfil its role, a VTS provides timely and relevant information to assist vessels in making informed decisions. This includes details such as vessel positions, identities, intentions and movements as well as Maritime Safety Information, reporting requirements and any limitations that may affect navigation. A VTS also cooperates with allied services to ensure efficient operations.

Beyond the provision of information, a VTS actively monitors and organises traffic. This may involve the planning of movements in advance, allocating space, issuing traffic clearances, advising on routes to be followed and ensuring compliance with regulations. Should unsafe situations arise, such as a vessel deviating from its route, experiencing equipment failure or encountering severe weather, a VTS responds by offering information, advice, warnings and instructions and by supporting emergency or other allied services where necessary.

The Global Navigation Satellite System (GNSS) is fundamental to VTS, providing position and timing data that underpins a range of operations, predominantly in the form of vessel tracking using the Automatic Identification System (AIS). Vessels use GNSS to determine their position and report it through systems such as AIS and equally a VTS uses the same data to monitor traffic and maintain situational awareness. The loss of GNSS will reduce the effectiveness of a VTS in monitoring and managing vessel movements.

A range of other internal VTS systems are supported by GNSS. Timing signals are often used to synchronise systems and correlate RADAR and AIS data.

GNSS may also support other systems within a VTS area which may include synchronised Marine Aids to Navigation (AtoN) lights in navigation channels or critical areas, the transmission through AIS of meteorological, hydrographic or other maritime safety information and the provision of data from virtual or synthetic AIS AtoN.

GNSS interference, whether through natural events, jamming or spoofing can therefore affect both external interactions with vessels, internal systems and some AtoN, increasing the risk of unsafe conditions.

Impact of GNSS Jamming and Spoofing on VTS

External VTS Interactions

Jamming

GNSS jamming could be localised or spread over a wide area and impacts the ability of vessels to transmit position data via AIS. Noting that a VTS is established due to the volume of traffic or the degree of risk, the areas that they cover are often at the most critical stage of a vessels passage and are generally amongst the most challenging to navigate.

As AIS and GNSS data are integrated into bridge navigational systems, any GNSS interference can affect both onboard decision making and the ship-to-shore interface. Bridge teams may experience confusion and VTS personnel may mitigate this by providing more frequent communication to maintain safety.

GNSS jamming also impacts AtoN that rely on GNSS for timing and positioning. Some AtoN require GNSS to synchronise light characteristics during setup and periodic re-synchronising in multiple locations and often navigationally significant areas. Synchronised lights may flash incorrectly if GNSS is not available for an extended period, reducing their effectiveness and the ability to maintain situational awareness.

AIS-based AtoNs, including virtual or synthetic aids, which may transmit meteorological or hydrographic data and other Maritime Safety Information, can reduce in effectiveness and utility should position information be lost or compromised.

Additionally, systems such as Portable Pilot Units (PPUs), will be impacted by the loss of positioning information which is critical in ensuring situational awareness for vessels operating in often confined and challenging waterways.

Spoofing

Spoofed GNSS signals can mislead VTS personnel into believing vessels are in incorrect locations. This compromises situational awareness and may result in unsafe routing decisions, increasing the risk of collisions, contacts or groundings. Spoofing may be more challenging to detect, particularly if it is localised or limited in nature where its impact may not be as readily apparent.

When spoofing occurs the position or speed of a vessel sourced from AIS becomes unreliable. The integrity of AIS data is essential for safe traffic management and spoofing undermines confidence. False or manipulated data presented to both VTS and vessels can influence the sharing of information impacting upon decision-making, creating confusion and potentially hazardous situations. This may include the sharing of digital information passed on from a VTS, for example to PPUs.

Internal VTS Technology and Personnel

Jamming

VTS systems rely on AIS data for traffic monitoring and when GNSS signals are disrupted, AIS-derived positions may become lost, freeze at the last known location or 'wander.' This compromises the integrity of the portrayal and makes it difficult for VTS personnel to understand the traffic image.

Additionally, trials have shown that equipment onboard vessels may react differently to jamming depending on equipment type and integration. Some AIS units fail safe by ceasing transmission, while others continue to report erroneous positions. This inconsistency in how AIS data may be presented during GNSS jamming creates uncertainty for VTS personnel.

For VTS centres, jamming can lead to unusual working conditions, multiple alarms and increased workload. VTS personnel must cross-check RADAR and other sensors manually to verify vessel positions which slows decision-making and raises the risk of human error. In ports and harbours, this loss of integrity in traffic information can disrupt normal operations, potentially cause delays and reduce confidence in automated systems.

Spoofing

GNSS spoofing also undermines trust in automated VTS tools and decision-support systems. When VTS personnel cannot rely on these outputs, they must introduce additional verification steps, such as cross-checking RADAR and manual reports, which slows interactions and responses during critical operations.

Spoofing can also compromise internal logs and operational records, creating uncertainty about the accuracy of historical data.

Safety Concerns

The knock-on effects of GNSS jamming and spoofing extend beyond technical disruption and have serious implications for the safety of navigation, operational integrity and human factors within VTS environments.

When GNSS signals are lost or corrupted, the integrity of the traffic image will become compromised forcing VTS personnel and bridge teams to rely on RADAR, other sensors, AtoN and voice communications, thereby influencing overall situational awareness both onboard and ashore.

The loss of GNSS timing can affect RADAR integration, AIS correlation, other VTS systems and decision-support tools. Individual VTS systems may behave in different ways during a spoofing or jamming event, which may include deleting tracks or, on the other hand, highlighting them. If a VTS is solely reliant on AIS data as the source of its traffic image, spoofing and/or jamming may be difficult to identify in the absence of other sensors, particularly RADAR, for verification.

The workload impact on both VTS personnel and bridge teams could be particularly high irrespective as to whether spoofing is over a wide geographic area or to a limited extent, as even with one vessel affected, the integrity of the whole traffic image may be undermined or questioned. This can distort the portrayal of information and compromise decision-support tools, reducing the effectiveness of safety-critical processes. In some cases, VTS may need to revert to infrequently utilised manual procedures and tools coupled with increased VHF communications which may all add to operational strain.

GNSS interference may affect wider AtoN provision. Synchronised lights may flash incorrectly and without accurate position information, AIS-based AtoNs may be missing or unreliable.

With compromised GNSS timing, the accuracy of databases and/or recordings may be undermined thereby presenting operational, commercial or legal difficulties.

Solutions

Mitigating the risks posed by GNSS jamming and spoofing in VTS operations requires a combination of technical measures, operational procedures, training and local, national and international collaboration. Organisations, such as IALA, highlight the vulnerability of GNSS and stress the importance of resilient PNT solutions.

Technical

A significant mitigation measure is the integration of sensors such as RADAR, AIS and CCTV to cross reference multiple independent sources to maintain a coherent traffic image during GNSS interference.

VTS providers are encouraged to conduct an analysis and determine which systems may be affected by GNSS interference and how. Early detection systems and alarms, along with training on the signs and symptoms, should be considered to provide early warning of jamming or spoofing events. VTS providers should determine if their VTS systems possess a jamming and/or spoofing detection capability and if so, understand and promote amongst personnel how it will behave in such cases.

A cost-effective solution may be comparing data from two GNSS receivers in known fixed locations. This comparison and authentication of known and fixed data may serve to provide an indication of jamming or spoofing.

Alternatively, shielded antennas can help block low-angle jamming or spoofing signals and emerging technologies such as signal authentication and encryption will make spoofing more difficult.

Terrestrial timing sources, where available, may provide a degree of redundancy to GNSS as a source of network and system timing.

Procedural

Authorities and VTS providers should consider GNSS interference in their risk assessments and as part of a Safety Management System (SMS).

Subsequent operational procedures should consider the provision of sufficient resilience and redundancy to maintain a RADAR and/or other sensor-based traffic image, coupled with enhanced voice communication and reporting procedures. In the event of jamming and/or spoofing enhanced VHF communication may be required to share traffic information and maintain situational awareness between ship and shore. With VTS

personnel now relying heavily on the benefits that AIS can deliver, coverage or tracking issues may go unnoticed. Recognising the increased reliance of AIS for vessel tracking, VTS providers should regularly verify the quality of non-AIS traffic images and conduct equipment capability checks and training to ensure readiness on a regular basis.

Local procedures should also address traffic management during GNSS outages. This may include reducing traffic flow, increasing separation between vessels or deploying additional pilots for critical passages recognising that support systems, such as PPUs, may be unavailable.

The presence of additional VTS personnel, including technical/engineering teams, may be required to manage increased workload during interference events. Mariners should be informed of GNSS issues by means of regular voice broadcasts or other means of Maritime Safety Information provision. Participating ships should also be required to report any GNSS interference experienced whilst transiting the VTS area and be aware of the responsibility and capability of a VTS to respond to developing unsafe situations.

A lack of situational awareness onboard may increase reliance on external systems, such as physical AtoN and charted features to create a common traffic image between ship and shore.

Training and Awareness

Training is critical to ensure VTS personnel can identify and respond effectively to GNSS interference. VTS personnel, pilots, bridge teams and other stakeholders should participate in regular exercises simulating jamming and spoofing scenarios. VTS personnel should maintain competence in their response to developing unsafe situations including, but not limited to, a vessel unsure of its route or position, deviating from a route, or requiring guidance to an anchoring position without the use of AIS information. These exercises could include RADAR-based monitoring and fallback procedures such as manual plotting.

VTS personnel should be trained to recognise signs of spoofing, such as sudden AIS position jumps or discrepancies between RADAR and AIS data. Familiarity with equipment settings for switching tracking sources is important.

Collaboration and Reporting

GNSS interference is a global issue and effective mitigation requires collaboration. VTS providers should report interference events to relevant local and national authorities.

In 2025 the IMO, ITU and ICAO urged States to protect GNSS operating in frequency bands allocated to the Radio Navigation Satellite Service (RNSS). They encouraged all parties to maintain conventional navigation infrastructure and develop mitigation techniques for such a loss. They also recommend issuing warnings to mariners when interference is detected and enforcing measures to prevent unauthorised transmissions on GNSS frequencies.

Relevant international organisations are encouraged to provide further guidance on GNSS interference, specifically tailored to VTS. States, competent authorities and VTS providers are encouraged to consult the IALA standards for guidance on VTS operations, technology and training.

Recommendations

To reduce the risks posed by GNSS jamming and spoofing in VTS operations, the following actions are recommended:

1. Technical Measures

- Consider installation of ant-jamming & spoofing equipment/systems.
- Integrate multiple sensors such as RADAR, AIS and CCTV to maintain a reliable traffic image during GNSS interference where possible.
- Regularly assess which VTS systems depend on GNSS and identify potential failure points.
- Assess all equipment that uses GNSS position and timing to understand the impact of interference.
- Consider installing and comparing data from two GNSS receivers in known fixed locations to provide an indication of jamming or spoofing.
- Consider installing detection systems and alarms to provide early warning of GNSS interference (including jamming or spoofing).
- Use shielded antennas to limit low-angle interference and consider technologies such as signal authentication and encryption to counter spoofing.

2. Operational Procedures

- Include GNSS interference as a risk in SMS procedures.
- Maintain competence and proficiency in voice communication procedures to share traffic information between ship and shore during outages.
- Verify the quality of non-AIS traffic images and conduct routine equipment checks including RADAR calibration to ensure readiness.
- Develop local procedures for managing traffic during GNSS interference, such as reducing traffic flow, increasing vessel separation or deploying additional pilots.
- Consider deployment of additional VTS personnel and technical/ engineering staff.
- Inform internal personnel and other stakeholders, as necessary.
- Issue warnings to mariners by means such as broadcasts when interference is detected and provide regular Maritime Safety Information.
- Ensure mariners are required to report to a VTS any GNSS interference experienced.
- Ensure vessels are aware of the ability of a VTS to respond to developing unsafe situations to assist in times of GNSS interference.

Training and Awareness

- Conduct regular exercises simulating jamming and spoofing scenarios.
- Train VTS personnel to recognise signs of GNSS interference such as sudden AIS position changes or discrepancies between RADAR and AIS data.
- Ensure VTS personnel are familiar with equipment settings, such as switching tracking sources and fallback procedures.

4. Collaboration and Reporting

- Report GNSS interference events promptly to local and national authorities and follow international guidance.
- Local, national and international organisations continue to provide guidance on GNSS interference in VTS areas.
- Consult IALA standards for best practice in VTS operations, technology and training.

VTS GNSS Interference Preparedness Checklist

Technical Measures

- Are multiple sensors (RADAR, AIS, CCTV) integrated to maintain a traffic image during GNSS Interference where possible?
- Has a dependency analysis been completed to identify which VTS systems rely on GNSS?
- Are GNSS interference detection systems and alarms installed or considered for early warning?
- Are shielded antennas fitted to reduce low-angle GNSS interference?

Operational Procedures

- Has GNSS interference been included as a risk in the SMS?
- Are voice communication procedures regularly practiced ensuring the provision of sufficient ship-to-shore traffic information during GNSS interference?
- Is the quality of non-AIS traffic images verified regularly?
- Are routine equipment checks (including RADAR) performed to ensure readiness?
- Are local procedures documented for GNSS interference scenarios (e.g., reducing traffic flow, increasing vessel separation, deploying additional pilots)?
- Is there a plan for deploying additional VTS personnel and technical/engineering staff during GNSS interference events?
- Are internal personnel informed promptly when GNSS interference occurs?
- Are warnings issued to mariners (e.g., broadcasts or Maritime Safety Information) when GNSS interference is detected?
- Are mariners required to report any GNSS interference experienced while transiting the area?
- Are vessels aware of the ability of a VTS to respond to developing unsafe situations and assist them during GNSS interference?

Training and Awareness

- Are regular exercises conducted simulating jamming and spoofing scenarios?
- Are VTS personnel trained to recognise signs of GNSS interference (e.g., sudden AIS position changes, RADAR/AIS discrepancies)?
- Do VTS personnel know how to switch tracking sources and apply fallback procedures?

Collaboration and Reporting

- Is there a process for promptly reporting GNSS interference events to national authorities?
- Is international guidance consulted and implemented?
- Are IALA standards consulted for best practice in VTS operations, technology and training?

Sources

IALA Guidelines

IALA (2025) *Guideline G1111-1: Producing Requirements for Core VTS Systems.* Available at: https://www.iala.int/content/uploads/2025/03/C02-10.4.3-Revised-Guideline-G1111-1-Producing-requirements-for-core-VTS-systems.pdf (Accessed: 5 December 2025).

IALA (2024) *Guideline G1129: Resilient PNT.* Available at: https://www.iala.int/product/g1129/ (Accessed: 5 December 2025).

Articles and Reports

IALA (2024) 'GNSS Jamming and Spoofing – Navigating Challenges in the Baltic Sea', *IALA e-Bulletin*. Available at: https://www.iala.int/e-bulletin/gnss-jamming-and-spoofing-navigating-challenges-in-the-baltic-sea/ (Accessed: 5 December 2025).

Britannia P&I (2024) 'Navigational Risks at Sea – The Growing Threat of GNSS Jamming and Spoofing'. Available at: https://britanniapandi.com/2024/10/navigational-risks-at-sea-the-growing-threat-of-gnss-jamming-and-spoofing/ (Accessed: 5 December 2025).

Risk Intelligence (2024) 'Maritime Navigation Under Threat'. Available at: https://www.riskintelligence.eu/analyst-briefings/maritime-navigation-under-threat (Accessed: 5 December 2025).

Marine Public (2025) 'GNSS Jamming Detection – Maritime Safety Guide 2025'. Available at: https://www.marinepublic.com/blogs/distress/710682-gnss-jamming-detection-maritime-safety-guide-2025 (Accessed: 5 December 2025).

Port Technology (2024) 'GPS Jamming Still Plagues Strait of Hormuz Traffic'. Available at: https://www.porttechnology.org/news/gps-jamming-still-plagues-strait-of-hormuz-traffic/ (Accessed: 5 December 2025).

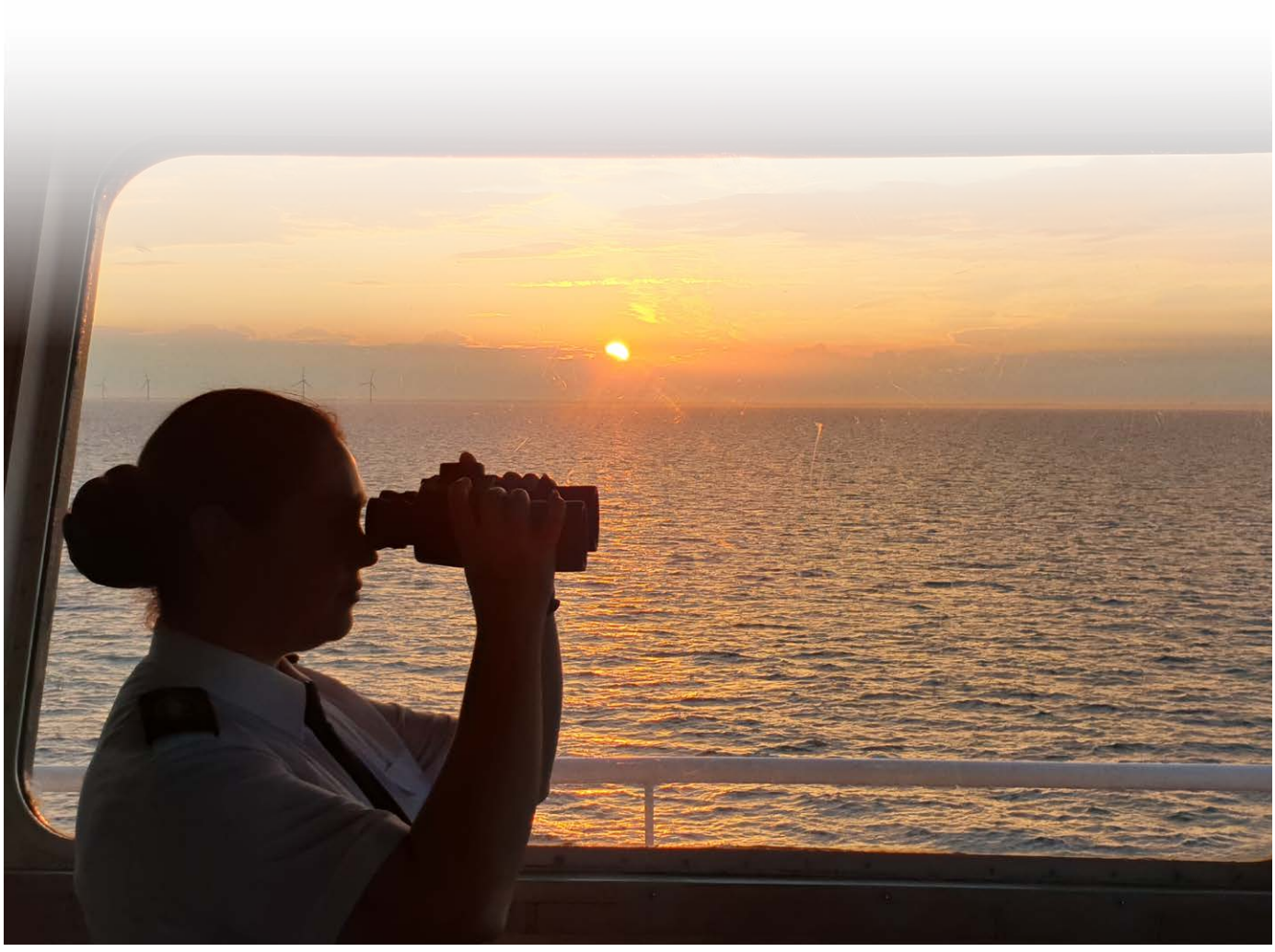
Hogg, S. (2019) 'GPS Jamming and the Maritime Industry', Port Technology International, Issue 46, pp. 68–71. Available at: https://www.porttechnology.org/wp-content/uploads/2019/05/PT46-09.pdf (Accessed: 5 December 2025).

UCL Discovery (2024) 'GNSS Vulnerabilities in Maritime Navigation'. Available at: https://discovery.ucl.ac.uk/id/eprint/10178187/ (Accessed: 5 December 2025).

Official Resources

U.S. Coast Guard Navigation Center (2025) 'Report a Problem'. Available at: https://www.navcen.uscg.gov/report-a-problem (Accessed: 5 December 2025).

NATO Shipping Centre (2025) 'Report GNSS Interference'. Available at: https://shipping.nato.int/nsc/page10303037 (Accessed: 5 December 2025).



Glossary of Terms

- **ADS-B:** Automatic Dependent Surveillance - Broadcast
- **AGC:** Automatic Gain Control
- **AIS:** Automatic Identification System
- **AtoN:** Aids to Navigation
- **BRM:** Bridge Resource Management
- **BNWAS:** Bridge Navigational Watch Alarm System
- **CRPA:** Controlled Reception Pattern Antenna
- **DP:** Dynamic Positioning
- **ECDIS:** Electronic Chart Display and Information System
- **eLoran:** Enhanced Long-Range Navigation
- **EPIRB:** Emergency Position Indicating Radio Beacon
- **EEZ:** Exclusive Economic Zone
- **EW:** Electronic Warfare
- **HDOP:** Horizontal Dilution of Precision
- **GMDSS:** Global Maritime Distress and Safety System
- **GNSS:** Global Navigation Satellite System
- **HF:** High Frequency
- **IBS:** Integrated Bridge System
- **IMO:** International Maritime Organization
- **INS:** Inertial Navigation System
- **LEO:** Low Earth Orbit
- **MF:** Medium Frequency
- **MOB:** Man OverBoard
- **MSI:** Maritime Safety Information
- **NAVTEX:** NAVigational TEleX
- **NAVWARNS:** NAVigation WARNingS
- **PNT:** Position, Navigation, and Timing
- **PPUs:** Portable Pilot Units
- **RADAR:** Radio Detection and Ranging
- **RIN:** Royal Institute of Navigation
- **SAR:** Search and Rescue
- **SART:** Search and Rescue Transponder
- **SATCOM:** Satellite Communications
- **SDR:** Software-Defined Radio
- **SOLAS:** Safety Of Life At Sea
- **SSAS:** Ship Security Alert System
- **VDR:** Voyage Data Recorder
- **VHF:** Very High Frequency
- **VMS:** Vessel Monitoring System
- **VTS:** Vessel Traffic Services

List of Reporting Authorities and Contact Information

- **US Coast Guard Navigation Center (NAVCEN):**
  - Online Report: https://www.navcen.uscg.gov/report-a-problem
  - Phone (24/7): +1 703-313-5900
- **NATO Shipping Centre (NSC):**
  - Email: info@shipping.nato.int
- **UK Maritime Trade Operations (UKMTO):**
  - Email: watchkeepers@ukmto.org
- **Joint Maritime Information Center (JMIC):**
  - Contact information as per latest advisories.

Impacts of GNSS interference on Maritime Safety.
A special report by the RIN GNSS Interference Working Group.

Digital Report Published January 2026.

V1.250126