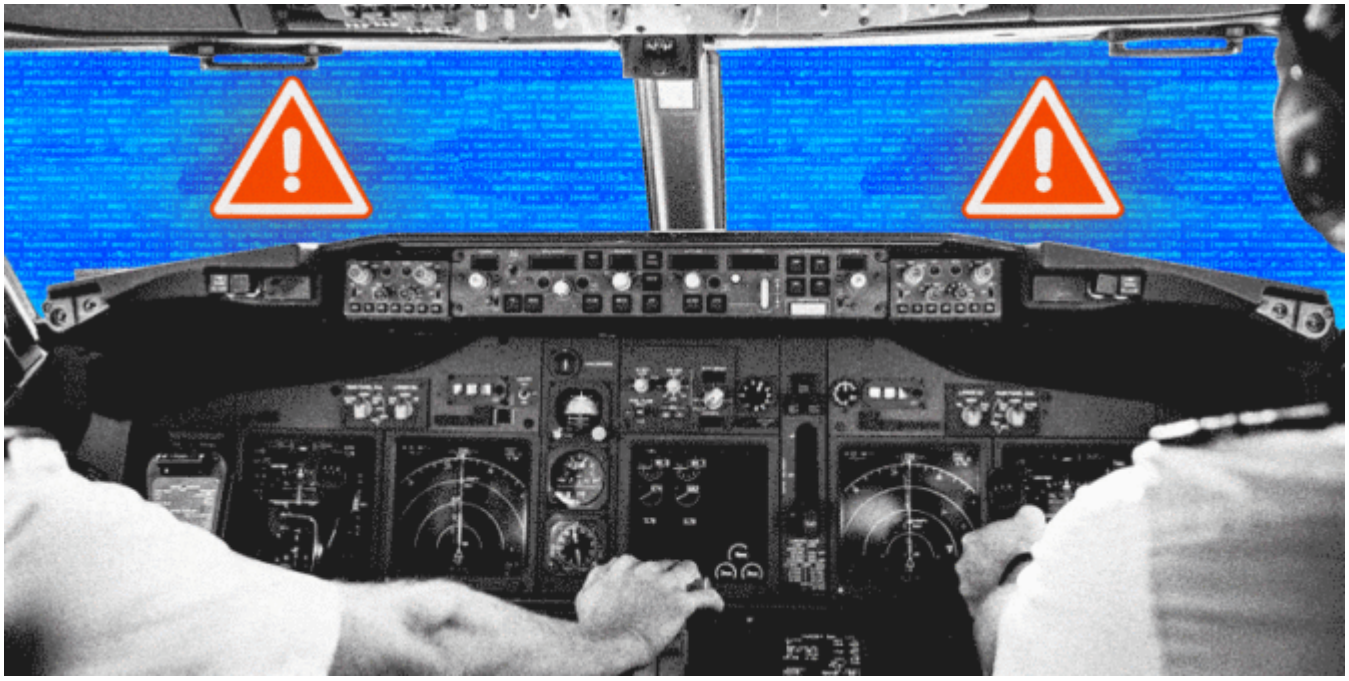
Spoofed Before the NAT? Here's What to Do

Chris Shieff
21 October, 2025



An OPSGROUP member on a recent westbound NAT flight from the Middle East received the following message via CPDLC:

The crew contacted Shanwick via HF, who requested their **RNP capability** and operational status.

The controller explained that due to their point of departure (OMAA/Abu Dhabi) they wanted to be certain the aircraft had not been **contaminated by GPS jamming or spoofing** before it entered oceanic airspace.

It's been a while since we wrote about this procedure, and since then we've had this NAT Ops Bulletin published by ICAO telling operators what to do on the NAT if they've experienced jamming/spoofing, so we reached out to NATS directly for an update. **Here's what they had to say…**

Defensive Measures

NATS reported they continue to receive a large number of flights every day that have been impacted by GPS interference prior to oceanic boundaries.

The issue is that once an aircraft's navigation system has been 'contaminated' by bad GPS data, it may not be possible to recover full RNP capability in flight, even if the normal GPS signal is restored.

These aircraft may no longer meet RNP 4/10 accuracy required in the NAT HLA, even **long after the trigger event occurred.**

The NAT Ops Bulletin which was published back in Jan 2025 requires crew of NAT-bound aircraft that have encountered GPS interference to notify their first NAT ANSP via RCL. Even if your aircraft shows no lingering effects, **ATC still want to know.**

NATS advise that late notification by pilots of a RNP degradation (such as approaching an oceanic entry point) greatly **increases controller workload.** They often need to move other aircraft out of the way to provide increased separation (in some cases from 14nm to 10 minutes), it's a big deal.

As a result, they are employing **defensive controlling measures.** Based on previously spoofed/jammed flights and regions of known risks, they may proactively contact flights assessed as higher risk to confirm status before entry – although the exact selection criteria isn't public. Increased separation will be applied until normal navigation performance is confirmed by the pilots.

In a nutshell, this is why the OPSGROUP member received the message above.

A special thank you to NATS for their help in answering this question.

Jammed or spoofed? You need to let your NAT ANSP know

The NAT Ops Bulletin we keep mentioning – this provides the guidance for NAT traffic on how to manage GNSS interference. Here it is again, so you can't miss it! ⬇

NAT OPS BULLETIN

Serial Number: 2025_001 **Issued: 7 January 2025**
Subject: NAT GNSS Interference Procedures **Effective: 7 January 2025**
Originator: NAT SPG

The purpose of North Atlantic Operations Bulletin 2025-001 is to provide background information and guidance to aircraft operators in the North Atlantic (NAT) on the requirement to notify ATC of GNSS interference, and the Air Navigation Service Provider (ANSP) procedures that will be applied to aircraft that have been exposed to Global Navigation Satellite Systems (GNSS) interference (GNSS jamming and/or spoofing) during their flight.

Any queries about the content of the attached document should be addressed to:
ICAO EUR/NAT Office: icaoeurnat@icao.int

NOTICE
NAT Ops Bulletins are used to distribute information on behalf of the North Atlantic Systems Planning Group (NAT SPG). The material contained therein may be developed within the working structure of the NAT SPG or be third party documents posted at the request of a NAT SPG Member State. A printed or electronic copy of this Bulletin, plus any associated documentation, is provided to the recipient as is and without any warranties as to its description, condition, quality, fitness for purpose or functionality and for use by the recipient solely for guidance only. The information published by ICAO in this document is made available without warranty of any kind; the Organization accepts no responsibility or liability whether direct or indirect, as to the currency, accuracy or quality of the information, nor for any consequence of its use. The designations and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

The NAT OPS Bulletin Checklist is available at www.icao.int/EURNAT/EUR & NAT Documents, NAT Documents, then NAT Ops Bulletins.

There is no objection to the reproduction of extracts of information contained in this Bulletin if the source is acknowledged.

NAT OPS Bulletin 2025_001_GNSS_RFI.docx Issued date: 07 January 2025

Key takeaway from this: If you suspect or know that your aircraft has encountered any kind of GPS interference (both jamming or spoofing), NAT-bound traffic must let their first NAT ANSP know in the RCL – even if the aircraft appears to have recovered.

This is prefixed by ‘ATC REMARKS/GNSS INTERFERENCE’ and must include details of any system degradations.

A few messages to keep handy are:

‘ATC REMARKS/GNSS INTERFERENCE NO IMPACT.’

‘ATC REMARKS/GNSS INTERFERENCE NO CPDLC/ADS’

‘ATC REMARKS/GNSS INTERFERENCE RNP 10 ONLY’

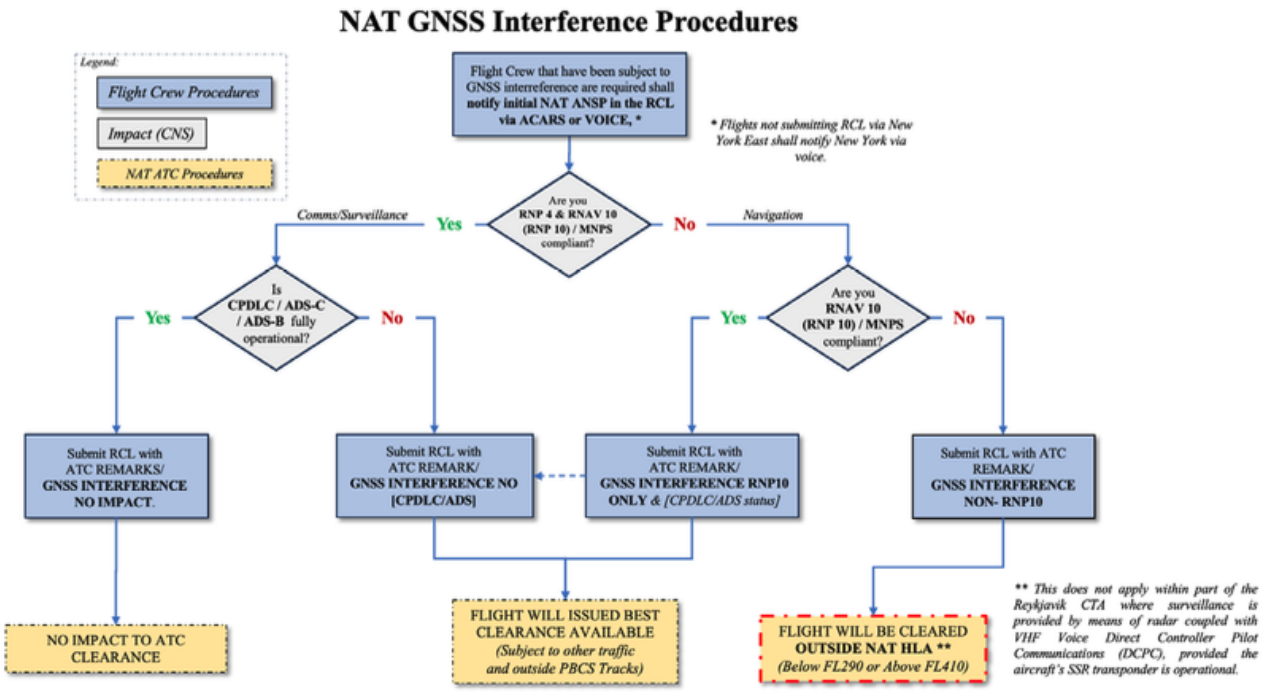
‘ATC REMARKS/GNSS INTERFERENCE NON-RNP10

By including your status in the RCL, you are **giving ATC a head’s up before you arrive.**

In most cases, you will still be allowed in the NAT HLA. A loss of RNP 4 isn’t a deal breaker, as you can still enter under RNP 10. But your clearance may be less optimal (likely level changes) due to the increased separation from other traffic.

The big one to look for is a loss of RNP 10. You will not be cleared into the NAT HLA, and instead will need to remain below FL290 or above FL410. With an obvious fuel impact, this may lead to an unplanned diversion.

The Bulletin includes a handy flow chart that’s worth printing and keeping in your flight bag.



Click for PDF.

Latest ICAO Feedback

The latest three-yearly ICAO Assembly was held in Montreal from Sep 23 – Oct 3.

During the event, ICAO issued its strongest condemnation yet of both **Russia and North Korea**, directly blaming them for **deliberate GNSS interference** in violation of the Chicago Convention. Russia, in particular, has been blamed by ICAO for **destabilising navigation across European airspace.**

We continue to receive regular reports from OPSGROUP members of both jamming and spoofing. Interference is now a regular occurrence in the **Baltic region, particularly around Kaliningrad, Eastern Finland, the Baltic Sea, and nearby airspace.** Other reports have been received from **Germany, Poland and Norway.**

Recent airspace incursions, airstrikes and drone activity associated with the **ongoing conflict in Ukraine** have almost certainly escalated the use of GPS interference as a defensive measure. Civil aviation will continue to operationally grapple with this hazard. **With no obvious solution in site, our best defence remains procedures like the one detailed above.**

US LOAs: What's the point of the C052?

OPSGROUP Team
21 October, 2025

Someone asked us about C052. Here's the answer.

Do you need it?

Well, my friend, to answer that you will need to answer these:

1. Are you Part 91, registered in the US?
2. Do you want to fly approaches that uses GPS RNAV stuff?
3. Do you want to fly these outside the US National Airspace System?

If you answered 'yes' to the above 3 then you probably need a C052

Are you now wondering *'Why exactly do I need it?'* or *'I have no clue about the C052!*"?

If you answered yes, read on. If you answered no, then move on.

Tell me about the C052

The C052 is a LOA.

In fact, it is *'an optional LOA provided upon the request of part 91 operators in order to show evidence of authorization and training to conduct Area Navigation (RNAV) Global Positioning System (GPS) approaches should they be required to provide such evidence to a civil aviation authority (CAA) outside of the United States.'*

So you need C052 if you want to **fly RNAV GPS approaches outside of the the US**, in countries where approval from your home state is required. Like anywhere that falls under EASA for example.

The C052 tells foreign authorities that you are trained and approved to fly GNSS based approaches, and this keeps them happy.

Hang on, do I actually want to fly GNSS based approaches?

Well, take a look at airports you visit and see if they have the following –

- A non-precision approach without vertical guidance, like an LNAV or an LP?
- An approach with vertical guidance like an LNAV/VNAV or LPV?
- A GLS approach?
- Titles which say RNAV (GNSS) or RNP approach?
- PRM?

Ok, then yeah, C052 is still for you.

I don't fly to Europe though. So where else do I need it?

Europe is the main spot, but there are others as well. **Hong Kong** for example. This LOA will allow you to fly them **anywhere that authorisation is required.**

One of the best ways to confirm is on the approach charts (it might say authorisation required) or in the Country Rules and Regs.

The UK used to have more stuff like **LPV approaches**, but since the UK lost access to EGNOS after Brexit, these LPV approaches haven't been possible.*

**Good news here though – Inmarsat have recently run tests on the new satellite system stuff that will replace EGNOS access for the UK. Watch this space for LPVs again. And C052 requirements for the UK. We aren't sure yet if it will be needed (it wasn't in the past).*

Something else to know about it.

The older LOA C052 used to mention LOA B034, but this is now out of use.

Because you also don't need approval to fly RNAV GPS approaches in US airspace, the best way to confirm your aircraft is eligible and airworthy for C052 stuff is **through your airplane flight manual** (from the manufacturer).

You might also want to get the C052 if you want a C073. **The C073 authorises you to use MDA as a DA/DH**, and you gotta have the C052 to get the C073

These guys can help.

Aviation Manuals can help you actually get the LOA if you want. We've mentioned them before, and actually they've mentioned the subject of C052 LOAs before, so here's a link to that.

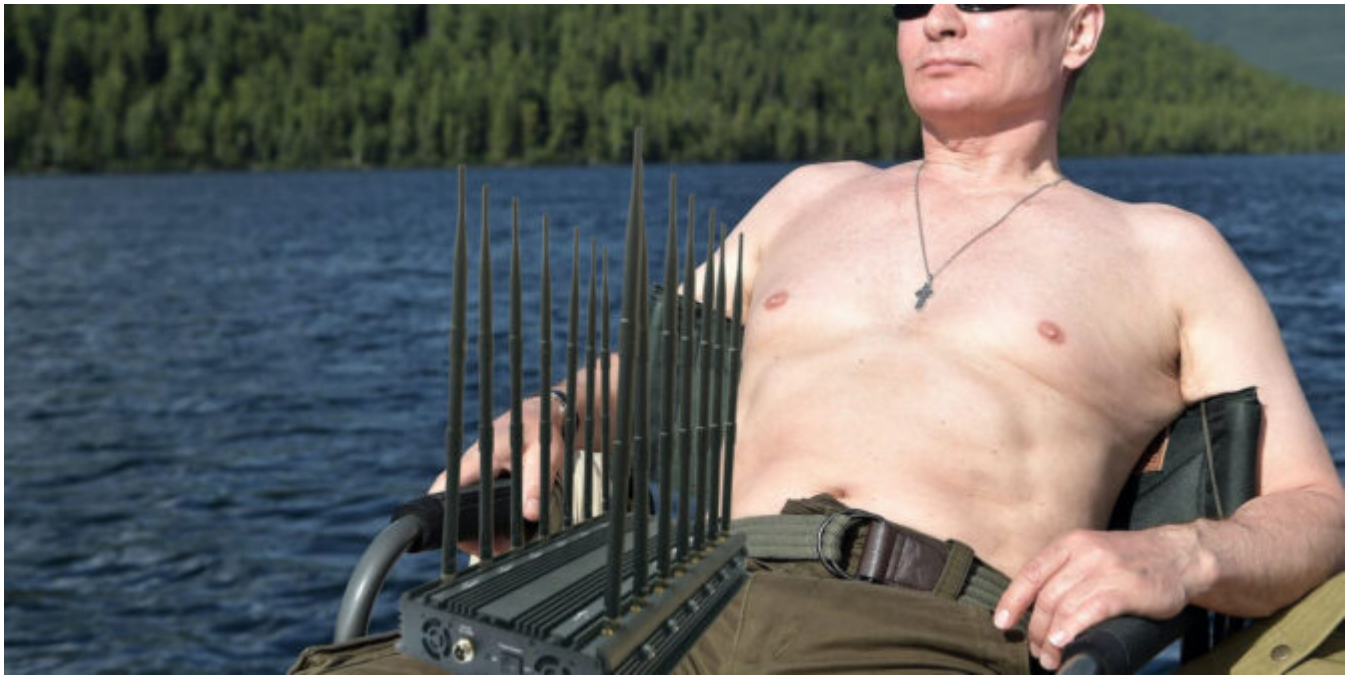
I'm sure there are other places who can help too, we just happen to find these guys really helpful because they always answer our questions on stuff.

Some useful other things to read.

- The FAA advisory circular.
- An FAA notice about the C052, effective May 2022.
- A post about LOAs – a quick rundown of what each one is for.
- Another post about LOAs – a guide on getting your LOA approved.

GPS Jamming: All the Wrong Signals

Chris Shieff
21 October, 2025



We live in a GPS world. This fantastic technology has **revolutionised aviation** since the first basic unit was approved for IFR use back in 1994. It has become engrained in day to day operations. We use it for a bunch of really important stuff – navigation, communication, surveillance, ADS-B and even TAWS. It is a technology that we rely on to stay safe.

And herein lies the problem. It relies on radio signals from satellites to work, and they can be **intentionally interfered with**. If you operate between Europe and Asia then the chances are this is not new. What is concerning is that it is happening more and more. In the last five years EUROCONTROL report that cases of GPS outages have risen dramatically. The number one suspect? **Deliberate interference.**

The Hot Spots

Almost always, widespread GPS outages occur in areas of political tension. It's no surprise then that the **Eastern Mediterranean, Middle East and Caucasus** are consistently the most affected regions – last year alone there were 3,500 reports of outages there. **About 10 a day**. And that's just from the people who spoke up. The **LCCC/Nicosia FIR over Cyprus** extending through to **LLBG/Tel Aviv** is particularly bad, with reports as far north as Italy, as well as **Turkey and Egypt.**

It is a part of the world **alive with tension** – spill over from the Syrian War, ongoing conflict in Libya and the current Azerbaijani conflict. Unfortunately it is also a **major air corridor** for flights between **Europe** and the **Middle East and Asia**. It is almost unavoidable.

But it's not just there – There are reports of GPS sabotage throughout the world – rings of interference (also known as 'crop circles') have been traced to **China, North Korea** and even **the US**.

So why tamper with GPS?

Unfortunately **electromagnetic warfare** is real. The goal for military interests is to make things as

difficult as possible for the other side including disrupting communications and navigation. GPS jamming is also used as a defence against drones – the explosive ones which we see in the headlines, and the ones that are spying. In other cases, jamming is used to protect people's **privacy**, and sometimes as a source of **criminal mischief.** Unfortunately for us, whether we like it or not, civil aviation is along for the ride…

Jamming or Spoofing?

GPS signals are low power, which means that a **weak interference** source can cause a receiver to fail, or more concerningly **produce false information**. A basic way to achieve this is with jammers – devices that mask the signal with noise. Although they are illegal in the US, they're not in other countries. And they're readily available.

A more sophisticated approach used by the military is '**spoofing**' where a ground station transmits a **fake GPS signal** that overrides the legitimate one.

In simpler terms – **jamming causes the receiver to die, spoofing causes it to lie.**

In powerful military applications, the effect of a single device has been known to affect a **300nm radius,** and it is almost impossible to locate them. They can be installed at bases, mounted in vehicles or put onboard ships.

So why is this a problem for aviation?

The issue is getting worse, and outages are sporadic and unpredictable. Three quarters of GPS loss worldwide is occurring in the cruise, and in ten percent of these cases it lasts for **more than half an hour.** There have also been reports where GPS receivers never regained a signal. According to ICAO's rules, frequent outages must be Notamed but the reality is, **few states are actually doing it.** To make matters worse, with so few aircraft flying during the pandemic it is unclear just how bad it is getting.

For crew, a loss of GPS forces an aircraft to rely on other means to navigate in airspace that **relies on accurate navigation** to separate you from other traffic. It can also lead to other issues including false alerts and even GPWS warnings. Requiring pilots to ignore them is a concerning precedent.

The plot thickens, enter 5G.

We've all heard about it – the revolutionary technology that will let you download your favourite episode of 'The Bachelor' in record time. Worrying news in the US has emerged that the federal government has allowed a new network provider to access a slice of the radio spectrum **usually reserved for GPS signals** to power a huge 5G network across the country. The frequencies are powerful, and there is **no guarantee** that they won't won't interfere with GPS signals.

So what can we do it about?

Unfortunately, like Covid, **the problem isn't going away anytime soon.** While manufacturers work on new ways to protect your aircraft, there are a few things you can do.

The most important thing is contingency – **have a plan.** Be aware of the threat of jamming if flying in affected areas of the world, and the issues it may create for you in the flight deck. If you lose GPS signal, **report it to ATC.** The more reports they get, the better. They will work to increase your separation and coordinate with other units.

When you're flying a GPS-based approach, know what you'll do if the **screen goes blank**. Be prepared for the unexpected because as recent events have shown, that super reliable technology can fail.

And **stay informed**, here are some useful resources:

- EUROCONTROL – check out the latest stats on GPS outages here, and report loss of signal here.
- FAA – GPS Anomaly Reporting Form. For all US based GPS issues.

GPS Jamming at Cairo

Declan Selleck
21 October, 2025

Egypt notified airlines yesterday that GPS jamming is a concern to arrivals and overflights, and warned against conducting RNP/RNAV arrivals or approaches.

The jamming was announced on 24MAY, and is centred on Cairo Airport; the source is unknown.

Similar GPS jamming was conducted, at state level in that case, by North Korea last month, from five locations along the border with the South. South Korea, along with other Civil Aviation Authorities, are looking at an eLORAN based alternative as a backup.

Operators planning flights through the Cairo FIR should monitor NOTAMs for latest.