

GPS Interference

Mains syllabus: GS3 - Science and Technology- developments and their applications and effects in everyday life, disaster management.

Why in the news?

Recently, GPS interference has emerged as one of the biggest challenges for seafaring vessels and aircraft.

What is GPS interference?

- **Global Positioning System (GPS)** - It is a space-based radio-navigation system, owned by the U.S. Government and operated by the United States Air Force (USAF).
- It can pinpoint a 3 dimensional position to meter-level accuracy and time to the 10-nanosecond level, worldwide and 24/7.



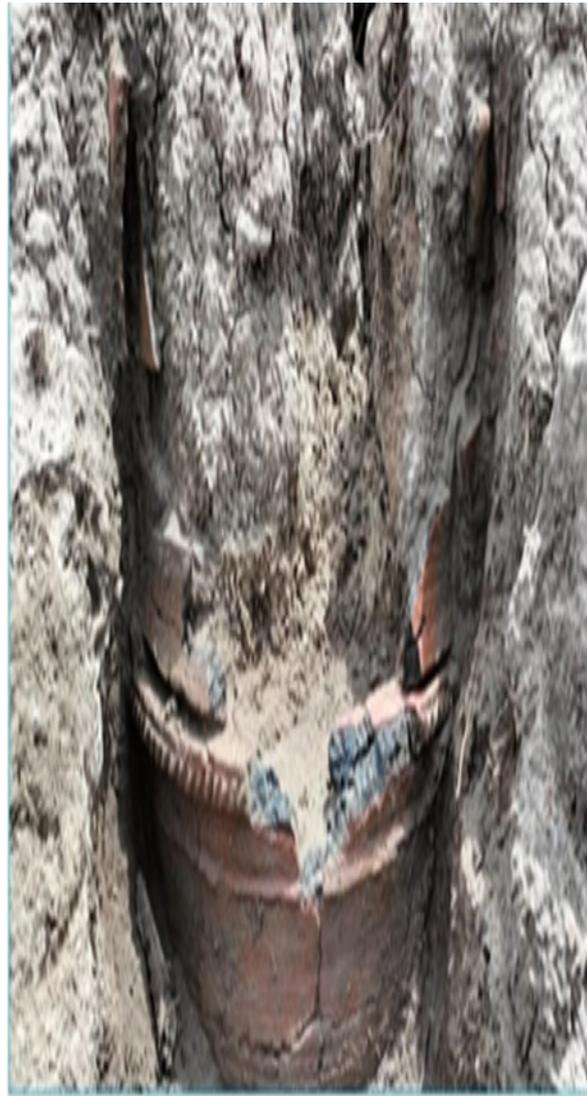
- **GPS Interference** - It refers to spoofing or jamming, two types of deliberate cyber-attacks on GPS signals, which disrupt or deceive vehicles' navigation systems.
- While both are often used synonymously with each other, spoofing and jamming refer to slightly different.

GPS jamming	GPS spoofing
Involves a device (jammer) emitting strong radio signals on GPS frequencies to <u>overpower weaker signals</u> .	Involves a device transmitting signals on the same frequencies used by GPS satellites, <u>blocking the GPS receivers</u> from acquiring or maintaining the right satellite signals.

It disrupts the functioning of GPS systems by *rendering receivers unable to determine location or time.*

Unlike jamming, which disrupts signals entirely, it *deceives the receiver into trusting false data.*

- **Causes** - GPS interference can occur due to various reasons, *not all of them malicious.*
 - Electromagnetic radiation from nearby devices
 - Adverse atmospheric conditions like ionospheric disturbances, solar activity (such as flares)
 - Intentional jamming/spoofing.



Why is it dangerous?

- **Disrupts military operations** - Spoofing can cause a pilot to *misjudge the aircraft's position*, increasing the chance of collisions with terrain or other aircraft.
 - In 2024, reports indicated up to 700 daily GPS spoofing incidents globally, highlighting the scale of the threat.
- **Interrupts civilian transport** - It can severely disrupt civilian transport by causing navigational errors, leading to *potential collisions, groundings, and traffic chaos.*
- **Disrupts maritime navigation** - It can also lead to *piracy, disastrous events.*
 - Persian Gulf and the Red Sea amid ongoing conflicts are one of the vulnerable regions.

Maritime tech consultancy Windward's Q1 2025 data show a 350% rise in **spoofing incidents in the Red Sea** alone compared to 2024—with some vessels having experienced sudden position jumps of hundreds of nautical miles.

- **Rising conflicts between nations** - If one nation suspects another of GPS interference, it can lead to accusations, *diplomatic tensions, and even retaliatory measures*, potentially escalating the situation.
- **Airspace avoidance** - For aircraft, spoofing is one of the primary risks of being in the airspace of countries in war.
- It forces the nations to immediately avoid these areas as a preventive measure.
 - **For example**, avoiding respective airspace during Russia and Ukraine conflict.
- **Navigation dependence vulnerability** - A mere dependence on GPS navigation is dangerous, if GPS interference happens, leads to *disruptions in daily operations and disasters*.
 - **For instance**, during the 1999 Kargil war and during in 2009 and 2012 Brahmos missile tests - US denied access to GPS.
- **Displays false information** - Leading to collision of ships, aircraft accidents, and civilian vessel crashes etc.

How it can be prevented?

- **Using alternative navigation systems** - Aircraft experiencing GPS spoofing mid-air can rely on other navigation systems like
 - **Inertial Navigation Systems (INS)** - It uses *gyroscopes and accelerometers* to track the aircraft's current position based on its last known location.
 - **VHF Omnidirectional Range (VOR) and Distance Measuring Equipment (DME)** - It provides ground-based radio navigation, allowing pilots to further cross-check their position.
 - **Instrument Landing Systems (ILS)** - They are critical for precision approaches during landing, are unaffected by GPS spoofing.
- **Enhancing crew training** - Pilots are also encouraged to listen carefully to the control room to pick up any chatter of suspected GPS spoofing and become immediately cautious of the possibility.
- **Employing alert systems** - Involving *sophisticated technology to alert* and take control of the aircraft/ships from auto-pilot mode to the manual mode.
- **Effective Use of terrestrial navigation** - It involves manual position fixing using land-based aids like lighthouses and radars, the immediate alternative to maintain situational awareness.

What lies ahead?

- *Diversifying navigation systems* can be to mitigate the risks of GPS interference in the future.
- *Multi-constellation Global Navigation Satellite System (GNSS)* systems can be adapted to mitigate against GPS interference.

Reference

[The Indian Express| GPS Interference Threats](#)

