



**Gary Kessler
Associates**

Training • Consulting • Research

GPS Jamming and Spoofing in the Aviation Environment

Gary C. Kessler, Ph.D., CISSP

Experimental Aircraft Association (EAA)
Daytona Beach EAA Chapter 288

17 September 2026
Port Orange, FL

whoami

Gary C. Kessler, Ph.D., CISSP
Gary Kessler Associates

- Retired Professor of Cybersecurity
- Guest Faculty, USCG Academy
- Fellow, USCG Auxiliary Cybersecurity Directorate (AUXCYBER)
- Advisory Board and Faculty, CyberBoat Challenge
- Advisory Board, Cydome

50GT Master/Assistance Towing
Master SCUBA Diver Trainer

+1 802-238-8913
gck@garykessler.net
<https://www.garykessler.net>



(c) Gary C. Kessler, 2017-2026

Acronyms and Abbreviations

ADS-B	Automatic Dependent Surveillance - Broadcast	PNT	Positioning, navigation, and timing
AIS	Automatic Identification System	QZSS	Quasi-Zenith Satellite System
ATC	Air traffic control	ROT	Rate-of-turn
ATON	Aid to navigation	SAFO	Safety Alert for Operators
CDMA	Code Division Multiple Access	SDR	Software-defined radio
CIA	Confidentiality, integrity, availability	SOG	Speed over ground
COG	Course over ground	SOLAS	International Convention for the Safety of Life at Sea
COTS	Commercial, off-the-shelf	UAV	Unmanned aerial vehicle
DHS	U.S. Department of Homeland Security	UHF	Ultra high frequency
DOT	U.S. Department of Transportation	USCG	U.S. Coast Guard
ECDIS	Electronic Chart Display and Information System	USN	U.S. Navy
EU	European Union	VHF	Very high frequency
FAA	Federal Aviation Administration	VTMS	Vessel traffic management system
GLONASS	Global'naya Navigazionnaya Sputnikovaya Sistema Глобальная навигационная спутниковая система	W	Watt
GNSS	Global Navigation Satellite System		
GPS	Global Positioning System		
IUU	Illegal, unreported and unregulated (fishing)		
LAX	Los Angeles International Airport		
LORAN	Long range navigation		
MEO	Medium Earth orbit		
MMSI	Maritime Mobile Service Identity		
NavIC	Navigation Indian Constellation		
NASA	National Aeronautics and Space Administration		

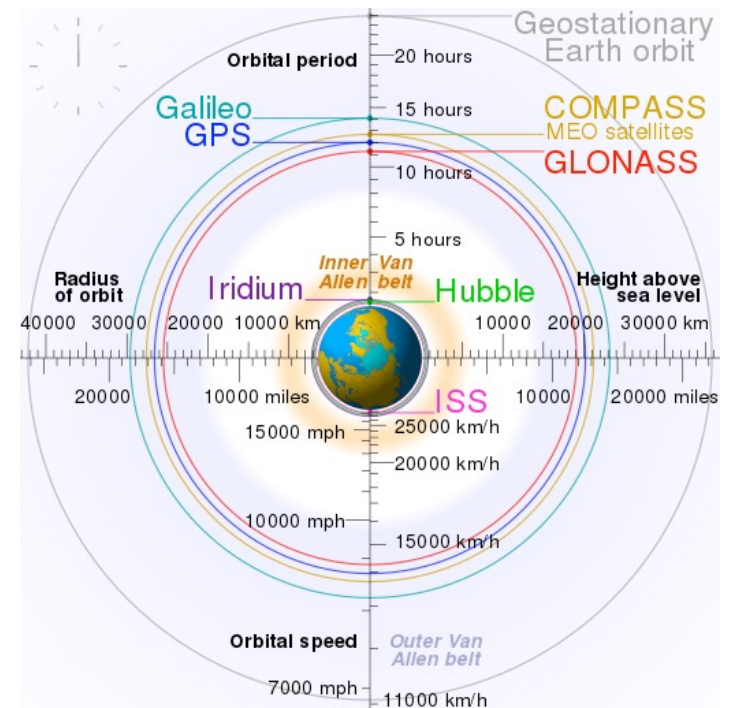
Overview

- GNSS and GPS basics
- GPS spoofing and jamming
- Example events in aviation
- Impact on aviation situational awareness: ADS-B
- Why spoof ADS-B and GNSS
- Conclusions

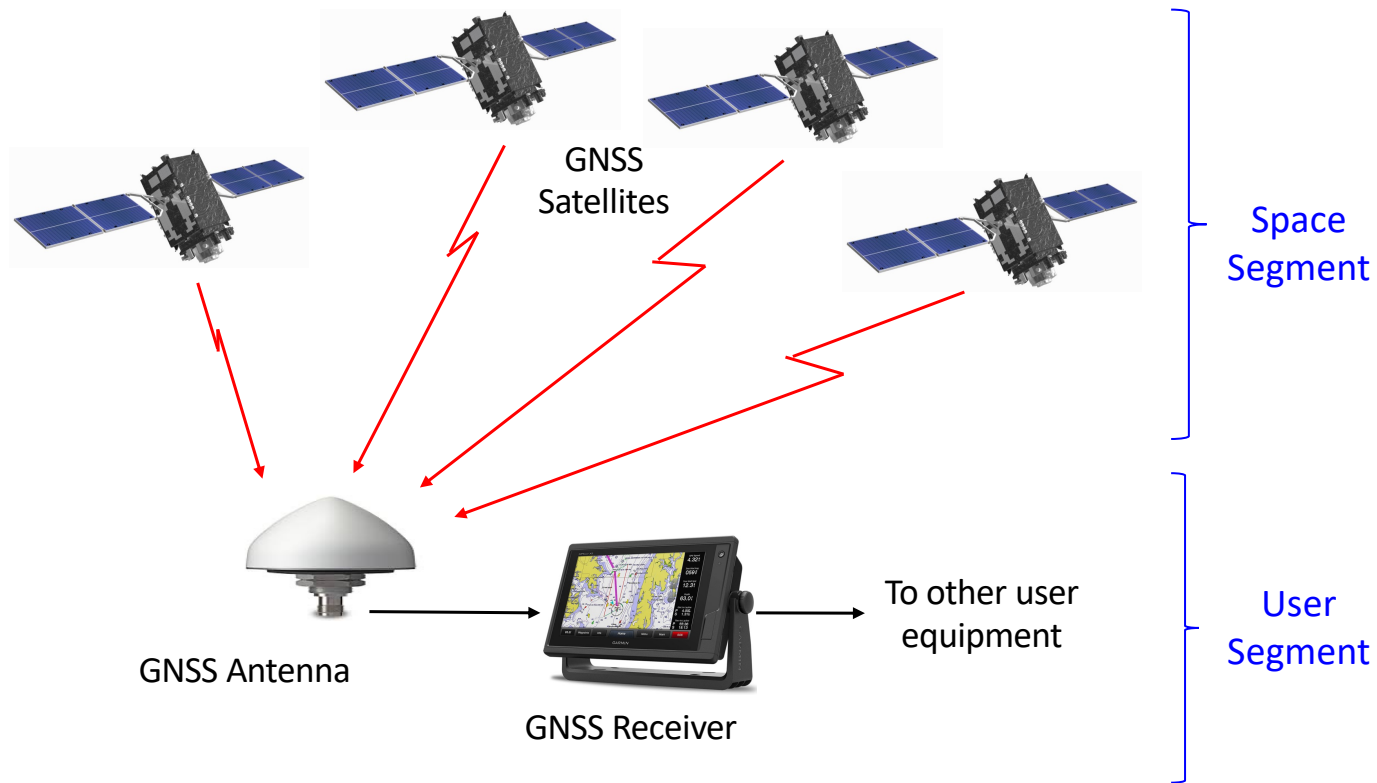


Global Navigation Satellite Systems

- Major navigation satellite systems
 - BeiDou-3 (China)
 - Galileo (EU)
 - GLONASS (Russia)
 - GPS (U.S.)
 - NavIC (India)
 - QZSS (Japan; aka Michibiki)
- Commonly employ 18-30 MEO satellites over several orbital planes
 - Altitudes range from 12-15K miles (19-23K km)
 - Periods range from 11-14 hours



Space and User Segments



(c) Gary C. Kessler, 2017-2026

GPS Control Segment

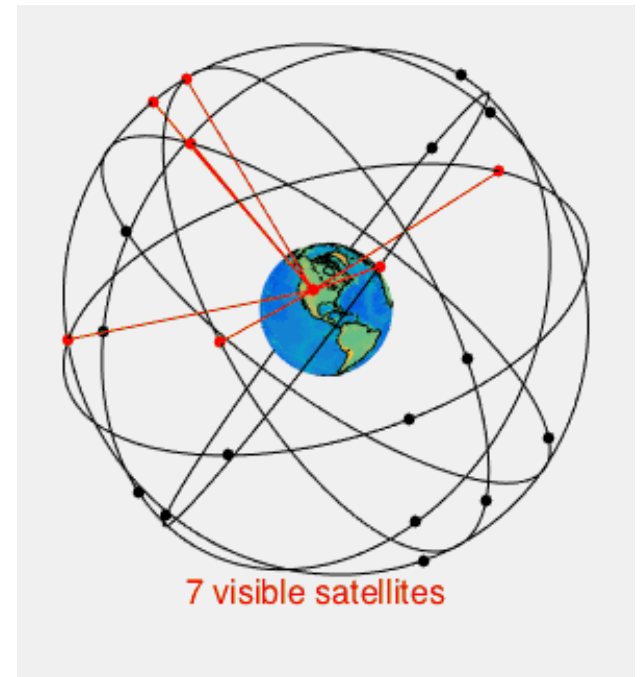


AFB: Air Force Base
AFSCN: Air Force Satellite Control Network
NGA: National Geospatial-Intelligence Agency
USNO: U.S. Naval Observatory

(c) Gary C. Kessler, 2017-2026

Space Segment Overview

- GNSS receivers determine position by trilateration
 - Passive range finding
- Transmissions in L-band (1-2 GHz)
 - Signals transmitted at 50 W, arrive at 10^{-16} W
 - Frequency sharing using CDMA
 - Each satellite assigned unique pseudorandom noise (PRN) sequence



A Word on CDMA...

- Code-Division Multiple Access (CDMA) is based upon frequency-hopping spread spectrum technology, invented in 1942 to aid USN torpedo guidance (rejected by Navy until 1960s!)
- Now used in Bluetooth, WiFi, mobile phones, and GPS



George Johann Carl Antheil



Hedwig Eva Maria Kiesler (aka Hedy Lamarr)
10th (and last) GPS III satellite named for her (2021)

(c) Gary C. Kessler, 2017-2026

Why Four Satellites?

- Satellites travel at 2.4 miles/sec (4 km/sec)
- Trilateration error can be 1 mile (1.6 km)
- Fourth satellite helps receiver correct clock drift (bias), reducing pseudorange error to 3 ft (1 m)

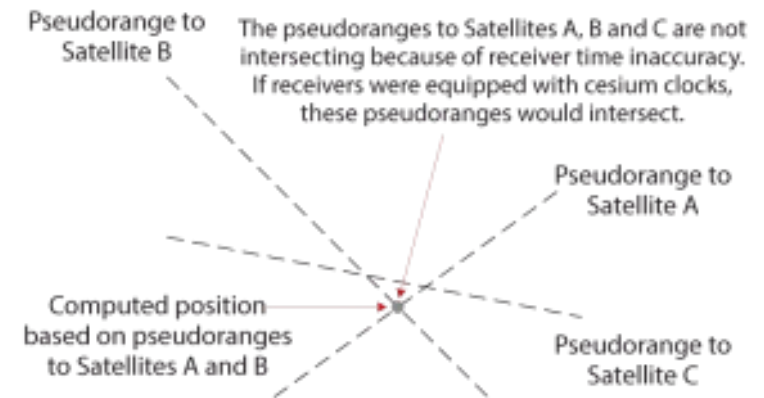
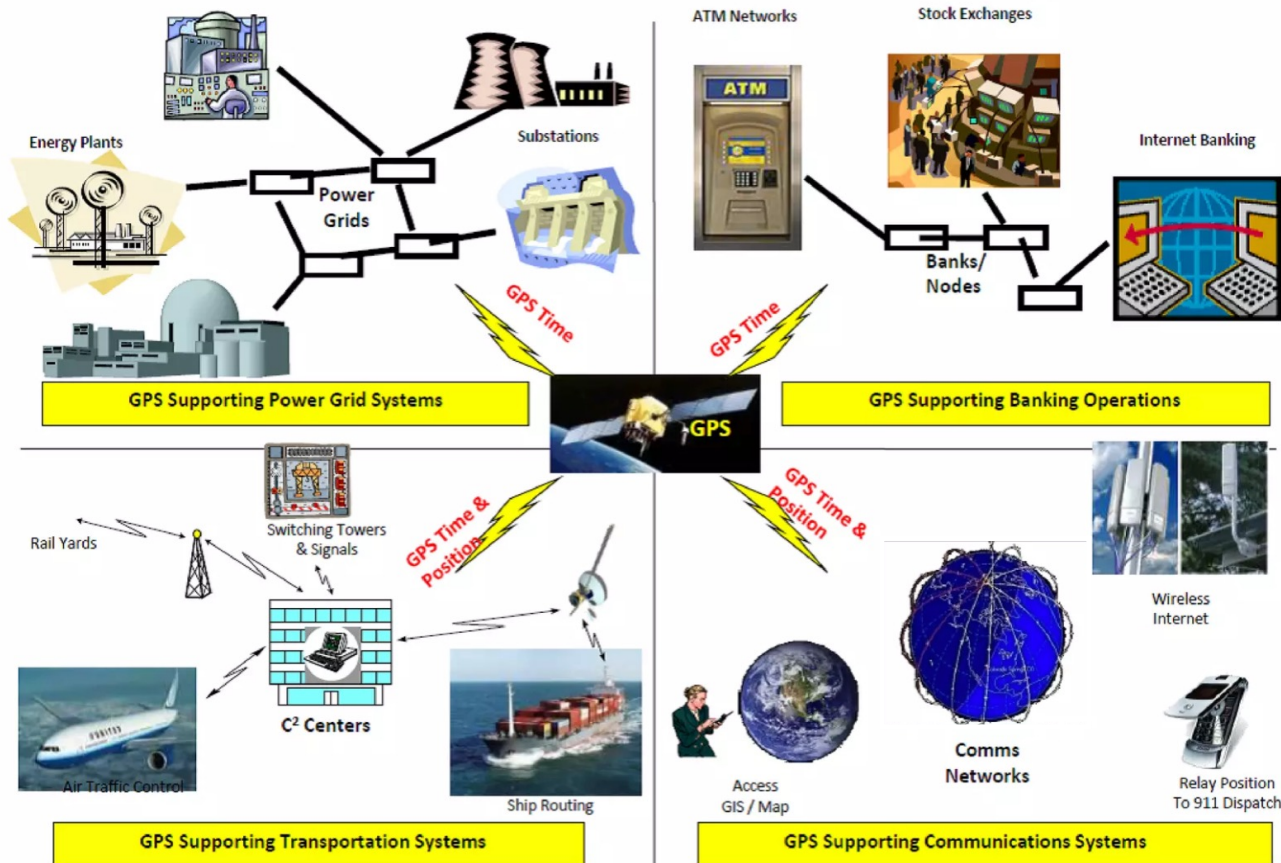


Figure 22 Detecting Position Error

NOTE: Satellites have cesium clocks, receivers do not!

GPS Timing and Critical Infrastructures



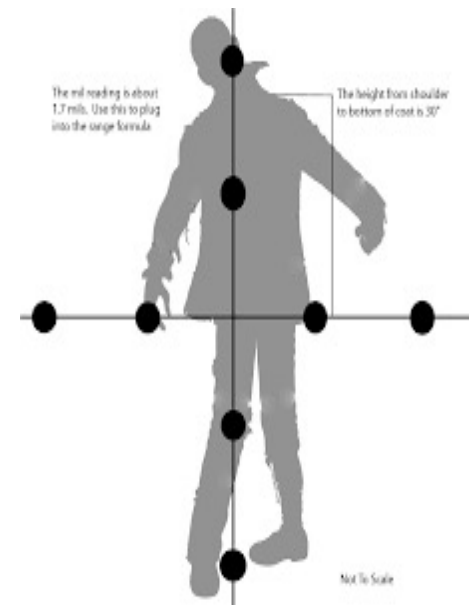
(c) Gary C. Kessler, 2017-2026

Case Study: Telstra Outage Due to Timing Fault

- Telstra suffers nation-wide network outage after timing failure (07/2026)
 - Several Telstra time server nodes — possibly Stratum-1 NTP nodes — reset clocks back to 11/2006, causing network outage
 - Calls, including those to 000, failed to complete
 - Train services, payment systems, public transport ticketing systems, and electric vehicle charging stations were also impacted
- Australia does not have a redundant, resilient national timing system, but relies on the Network Time Protocol (NTP) hierarchy

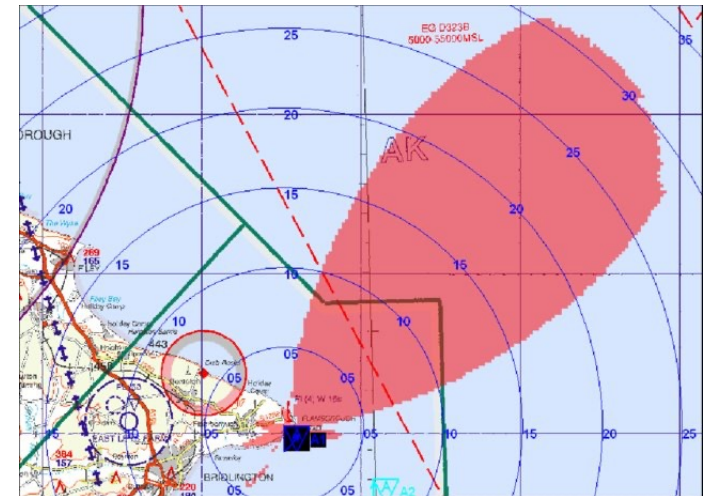
Side Note: GNSS Resiliency

- **Plug into the Formula Maxim:** Engineers don't understand security. They tend to work in solution space, not problem space. They rely on conventional designs and focus on a good experience for the user and manufacturer, rather than a bad experience for the bad guy. They view nature as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent.
- **Our systems — including GPS and other GNSS — are designed to be resilient against failure rather than attack**

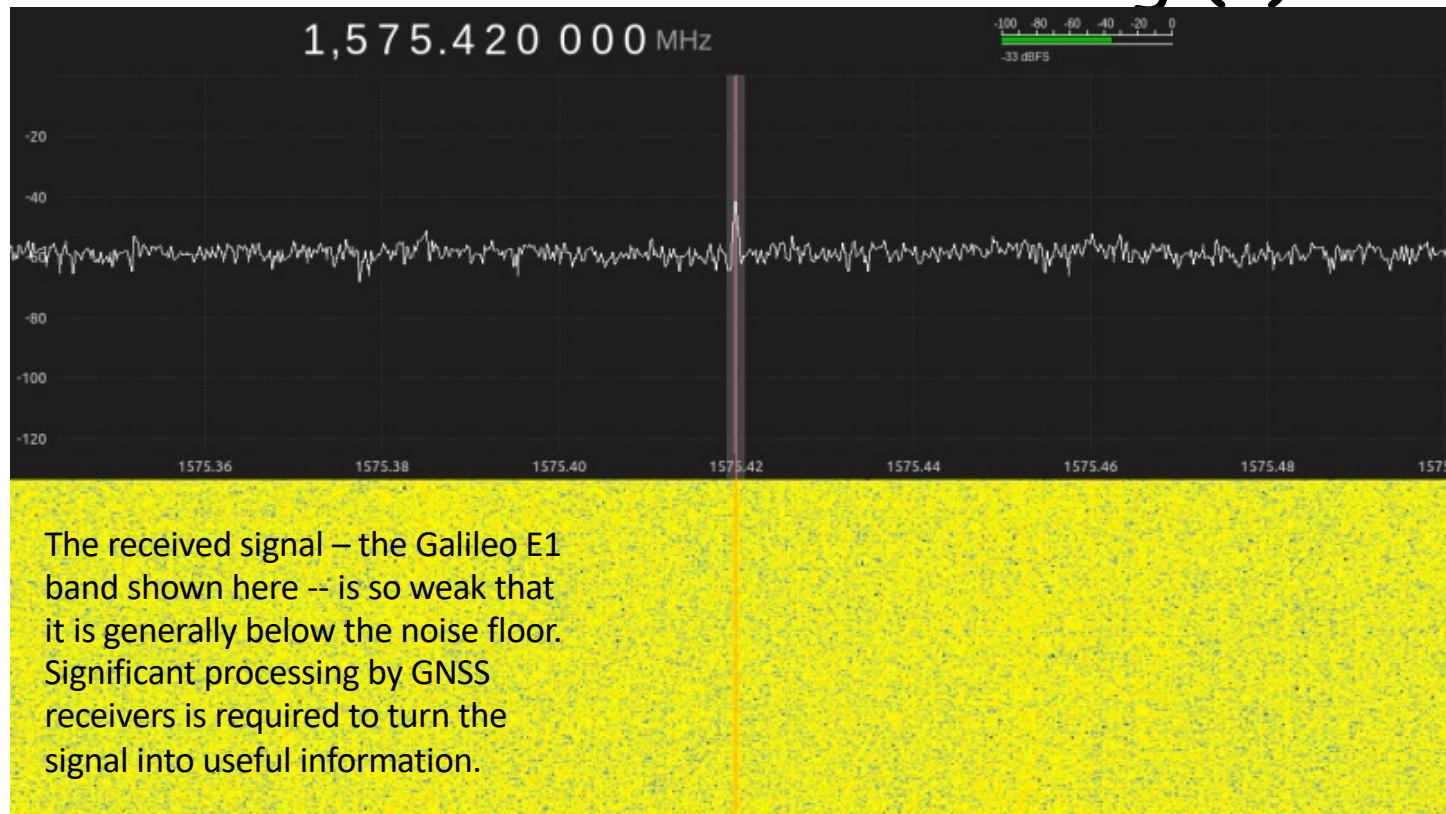


GPS Jamming and Spoofing

- *Jamming* is when an incoming signal is blocked so that a receiver cannot determine its position
- *Spoofing* is where a bogus signal is transmitted so that a receiver displays a false location

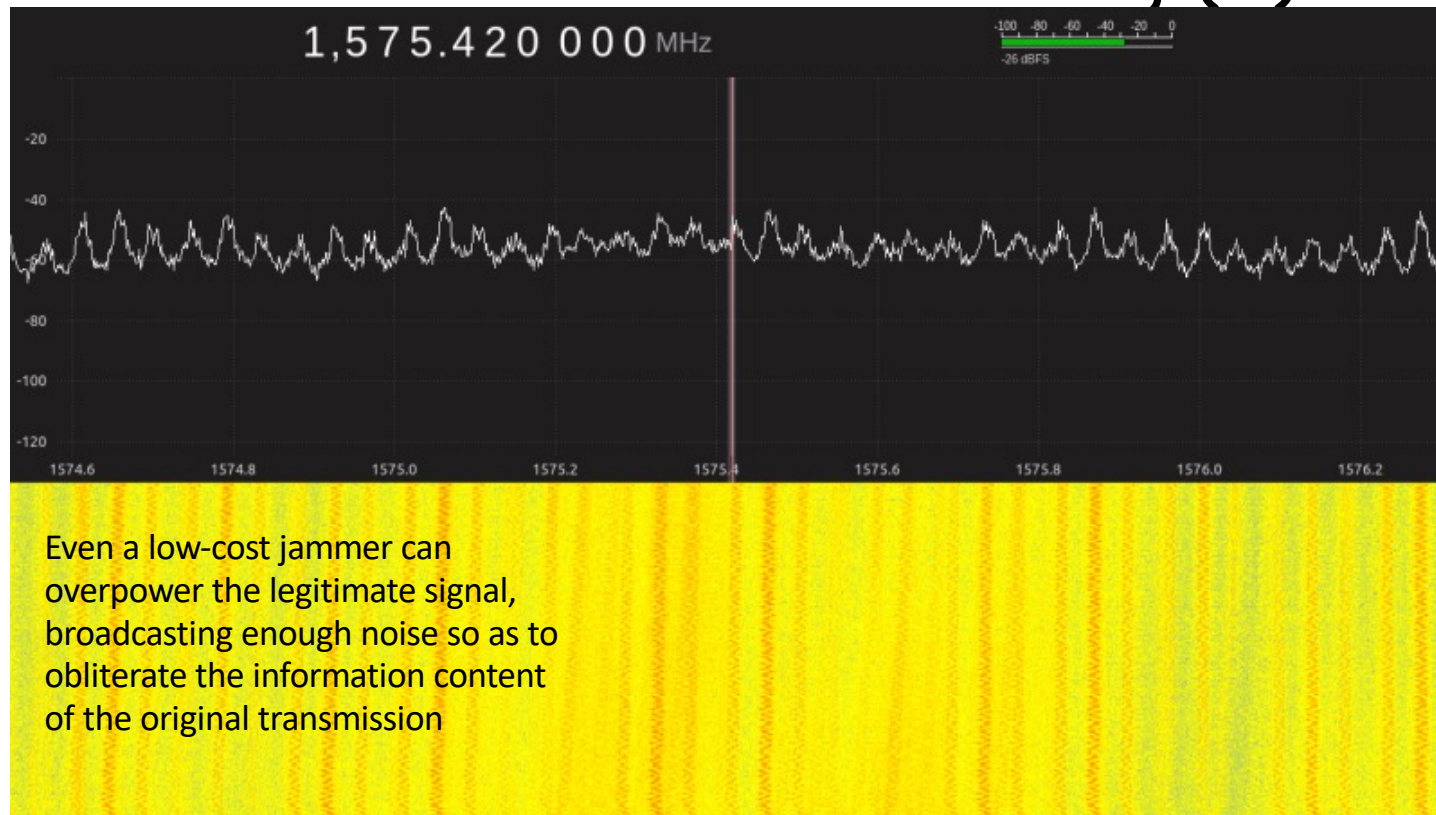


Side Note: GNSS Jamming (1)



(c) Gary C. Kessler, 2017-2026

Side Note: GNSS Jamming (2)



(c) Gary C. Kessler, 2017-2026

Only \$5.95 per month for your first 3 months

Get this deal ▶

audible

◀ Back to results



Roll over image to zoom in

Paddsun Car Anti-Position Satellite Signal Interference Jammer Shielding Instrument

Brand: Paddsun

★★★★☆ 11 ratings

Price: \$14.98

Thank you for being a Business Prime Member. Get \$200 off: Pay \$0.00 \$14.98 upon approval for the Amazon Business Prime Card with an eligible Prime membership. Terms apply.

Antenna	Satellite
Brand	Paddsun
Color	Black

About this item

- It can shield GPS satellite signals within the working range of 3-8 meters, All GPS terminal devices in the range will be invalid.
- The total transmission power is 0.3W, and the power loss is low, Easy to install
- NOTE: You must start the car before inserting the cigarette lighter to avoid burning the product due to the over-rated voltage
- Made of environmentally friendly materials, it will not cause harm to people.
- The machine can be removed immediately after use.

\$14.98

FREE delivery **January 3 - 5.**
[Details](#)

Or fastest delivery **December 30 - January 4.** [Details](#)

Arrives after Christmas. Need a gift sooner? Send an Amazon Gift Card instantly by [email](#) or [SMS](#).

📍 Deliver to Gary - Ormond Beach 32174

In Stock.

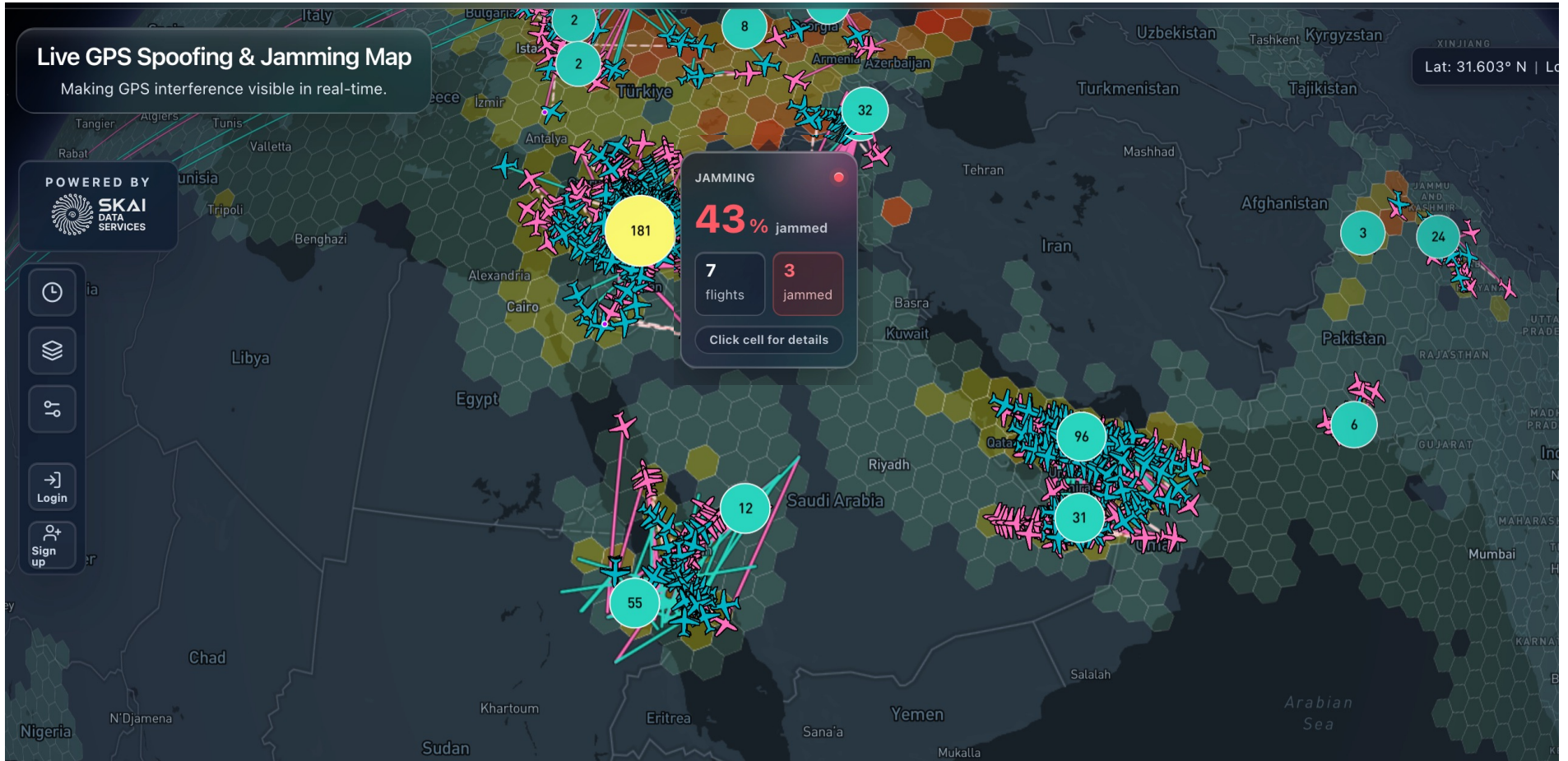
Qty: 1 ▼

Add to Cart

🔒 [Secure transaction](#)

Ships from and sold by [binweidianzi](#).

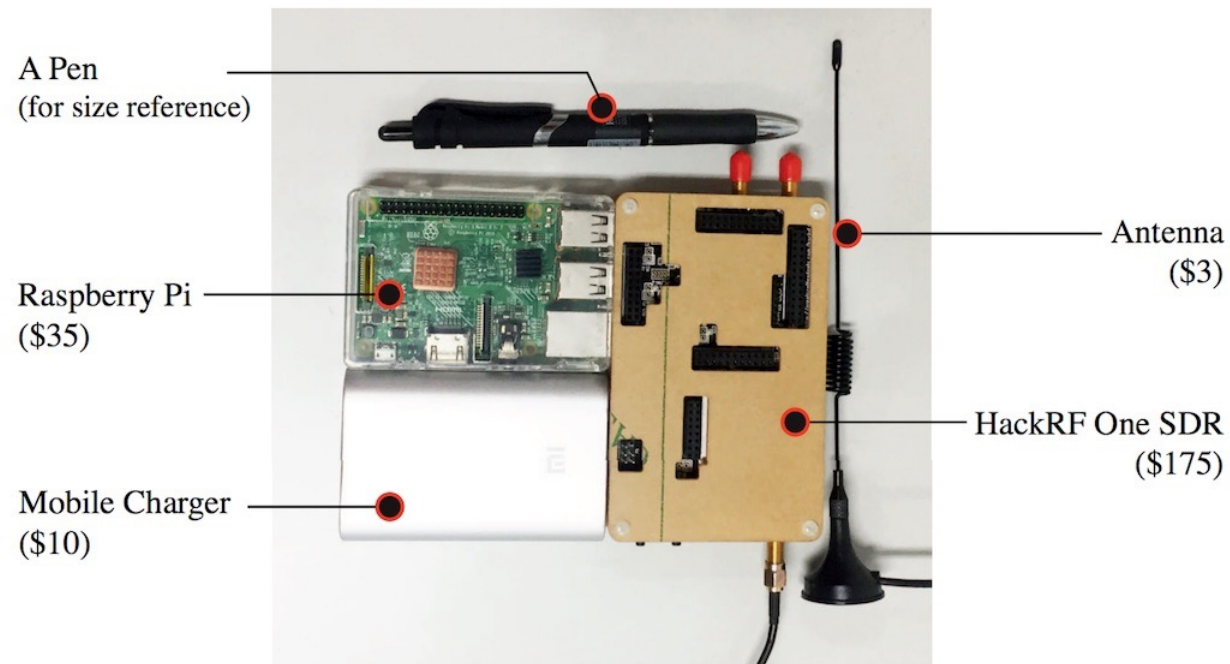
Add to List ▼



Case Study: GPS Spoofing Demo

- U. Texas, Austin team spoofed GPS signals to an Adaptive Flight Hornet Mini drone (06/2012)
 - Demonstration performed for DHS at White Sands Missile Range, NM
 - Drone hovering at 60' (18 m) received spoofed GPS signals from 3,300 ft (1 km) away indicating that it was climbing
 - In response, the drone started to dive to the ground
 - Spoofing employed \$1,000 COTS hardware and software that took UT four years to develop

Spoofing GPS With SDR (Hardware)



There are many similar devices;
this is but one example.

(c) Gary C. Kessler, 2017-2025

Spoofing GPS With SDR (Software)

GPS Spoofing with HackRF One

GNSS Spoofing with HackRF One and Jammer

1. SNR Monitoring

2. Coordinates Monitoring

3. PPS Phase Monitoring

Implementation Problems

System-level Protection

GNSS Spoofing with HackRF One, Jammer, and RF Amplifier

GNSS Spoofing with Synchronization. Deliberate Coherent Attack

GPS-SDR-SIM

GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as [ADALM-Pluto](#), [bladeRF](#), [HackRF](#), and [USRP](#).

Generating the GPS signal file

A user-defined trajectory can be specified in either a CSV file, which contains the Earth-centered Earth-fixed (ECEF) user positions, or an NMEA GGA stream. The sampling rate of the user motion has to be 10Hz. The user is also able to assign a static location directly through the command line.

The user specifies the GPS satellite constellation through a GPS broadcast ephemeris file. The daily GPS broadcast ephemeris file (brdc) is a merge of the individual site navigation files into one. The archive for the daily file can be downloaded from: <https://cddis.nasa.gov/archive/gnss/data/daily/>. Access to this site requires registration, which is free.

These files are then used to generate the simulated pseudorange and Doppler for the GPS satellites in view. This simulated range data is then used to generate the digitized I/Q samples for the GPS signal.

<https://github.com/osqzss/gps-sdr-sim>

<https://gpspatron.com/gnss-spoofing-scenarios-with-sdrs/>

GNSS Spoofing Mitigation

- Several methods can detect/mitigate GPS/GNSS spoofing
 1. Detect signal distortion at the instant that the bogus signal overpowers the legitimate signal
 2. Detects that the bogus signal is coming from a different direction than the legitimate signals
 3. Correlate the encrypted signal to ensure that it is authentic; even though the civilian unit cannot read the encrypted signal, it can ensure that it present
 4. Employ a GNSS receiver that can monitor multiple constellations
 - U-2 pilots reportedly use watches supporting all GNSS
 - Raymarine GA150 includes GPS/GLONASS receiver
 5. Implement some form of back-up (e.g., LORAN)



Garmin Instinct w/ GPS, GLONASS, and Galileo

GPS User Issue Detection & Evaluation (GUIDE) Tool

***Disclaimer:** These reports do not validate or verify any degradation to the GPS Constellation. This display and reports are derived from user submissions to the USCG Navigation Center GPS Problem Reports page. Size, range and intensity of the heatmap displayed is representative in nature only and does not represent real world impacted areas. To report a GPS Problem Report, click here: [Report a Problem | Navigation Center \(uscg.gov\)](#)

Note: the default view is the LAST 30 DAYS. Use the map menu to select a different time frame.



809	03/15/2025	Yanbu, Saudi Arabia	Marine	USER: Large GPS position offset occurred 290 NM from true position. Fault Unknown position recieved 19 06.6N / 037 14.2E, True position 23 55.0 N / 037 29.2 E. GPS speed variations occurred from 0 to 40 knots. One of the GPS receivers lost all satellites and HDOP 1. Disruption continues more than 1 hour. NAVCEN: The GPS Operations Center reviewed the GPS Constellation and Control Segment, there are no known anomalies that might affect GPS signal integrity at the time and vicinity of the reported problem. Space weather was reviewed and found unlikely to have impacted GPS performance. There were no authorized GPS tests in the area. No correlating reports from inter-agency partners. No additional information.	03/17/2025
-----	------------	---------------------	--------	--	------------

GPS and Aviation



(c) Gary C. Kessler, 2017-2026

GPS Jamming in Aviation

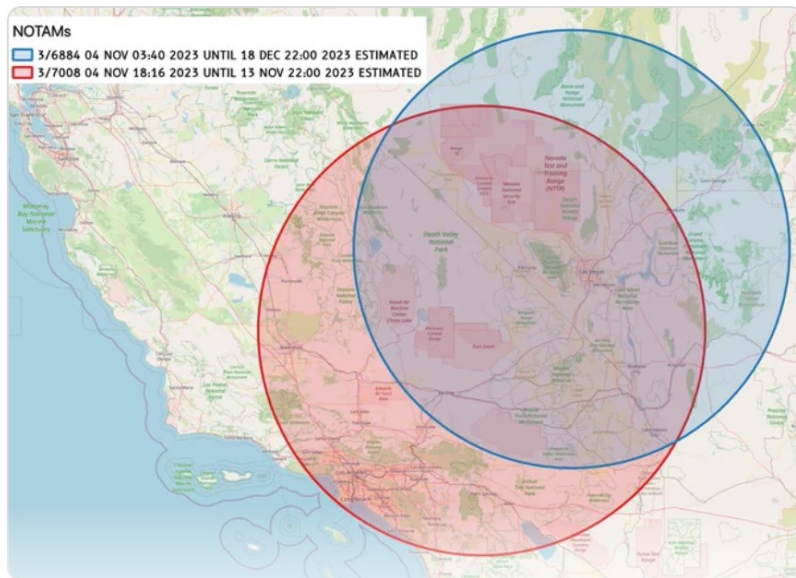
- Several incidents of GPS jamming occurred at Liberty International Airport (EWR) while tests were ongoing for new ground-based augmentation system (GBAS) (08/2012)
 - 1st Boeing 787 made GBAS Landing System capable landing in 10/2012
- GPS jammer found to belong to a truck driver who didn't want his company to be able to track his location at certain times on certain days
 - A truck on the New Jersey Turnpike ran with a GPS jammer between 03/2009-04/2011 before being caught

Early GPS Issues

- Between 2013 and mid-2016, ~80 reports of GPS signal interference or malfunction were reported to NASA
 - Reports from small to large aircraft, general and commercial flights, and countries from France and the U.S. to Egypt and Turkey
 - Majority of incidents were total signal loss or misreporting location



GPS Issues Continue Today...



NOTAM warnings about ADS-B/TIS-B/FIS-B/ADS-R being unavailable over Nevada and Southern California (John Wiseman on X)

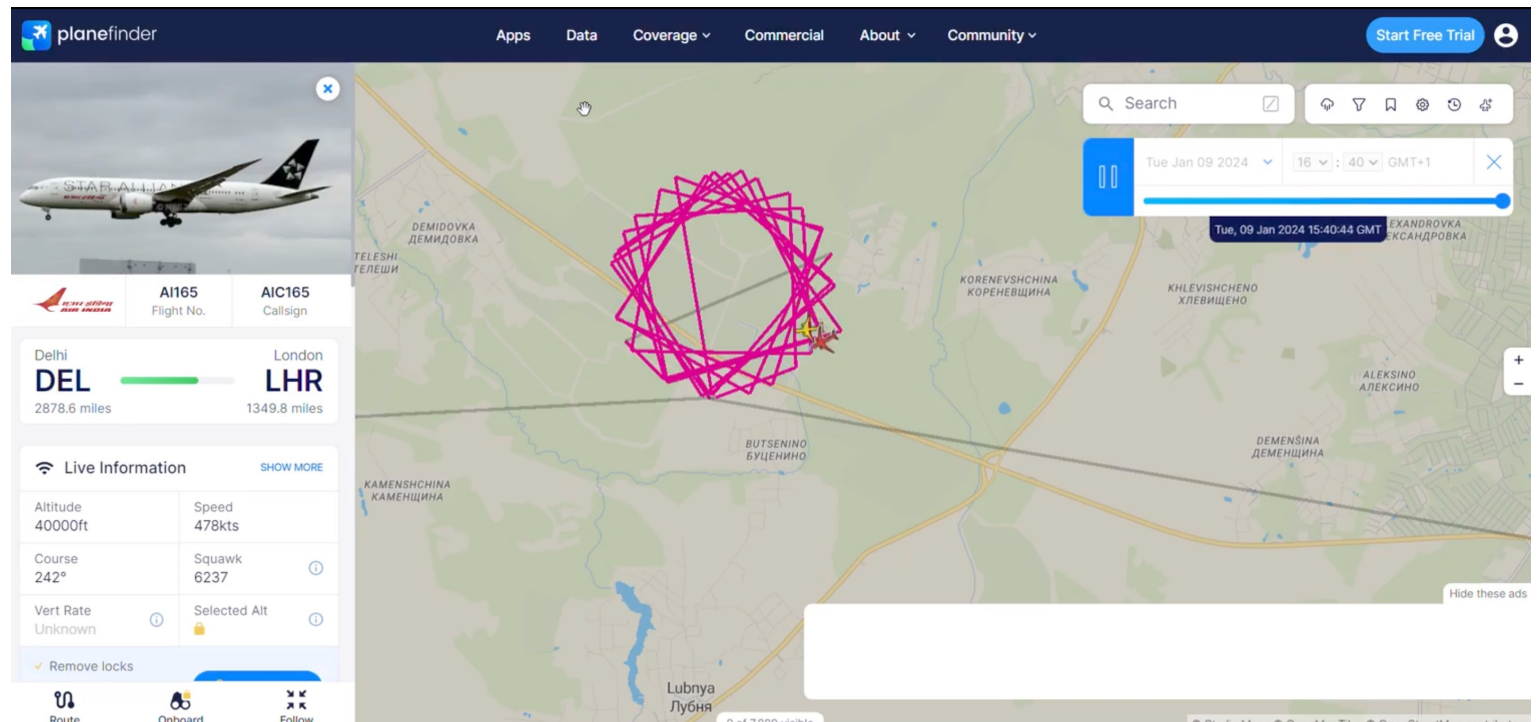


(c) Gary C. Kessler, 2017-2026

GPS Spoofing Squares

GPS square spoofing over Smolensk, Russia (01/2024)

Contrast with circle spoofing seen in maritime since 2019



(c) Gary C. Kessler, 2017-2026

Case Study: GPS Incidents in Aviation (1)

- Hannover Airport, Langerhagen, Germany (2012)
 - GPS repeater in a hangar — 3,300 ' (1 km) from runway — used to test receivers in business jets
 - Hangar door inadvertently left open...
 - Arriving and departed planes lost the real GPS signal, locked onto the hangar's signal, and received warning alarms and position-lost alerts
- El Paso International Airport, Texas (2020)
 - Commercial airliner lost GPS upon approach and required multiple approaches to safely land
 - Signal loss due to GPS disruption testing at White Sands Missile Range (New Mexico)



Case Study: GPS Incidents in Aviation (2)

- Friedman Memorial Airport (SUN), Sun Valley, Idaho (2019)
 - During period of low viz, plane cleared to descend to 9,000 ft. (2,743 m) on GPS-based instrument approach
 - Radar controller 250 miles (402 km) away noticed that plane was at 10,700 ft. (3,261 m) and approaching a 10,900 foot (3,322 m) mountain
 - Radar controller called control tower which vectored the plane in time to avoid a fatal crash
 - Local GPS interference due to military testing affected both the plane and local control tower
- NASA's Aviation Safety Reporting System (ASRS) contains >90 GPS interference reports in U.S. since 2012, most in 2019-2020
 - E.g., 21 GPS problem reports were made to FAA in one day near LAX (03/2018)



Case Study: GPS Incidents in Aviation (3)

- Denver International Airport (DIA) (2022)
 - Pilots reported safety concerns upon landing
 - Investigators took 33 hours to find and shut off source of interference
- Dallas-Fort Worth (DFW) (2022)
 - Jamming disrupted traffic and caused gate delays
 - Episode lasted 44 hours and source never found
- GAO report says that DOT should respond better to GPS jamming incidents (03/2023)



Case Study: Jamming Passenger Flights

- Chinese Warships Suspected of Signal-Jamming Passenger Jets (03/2023)
 - Qantas Airways warns about ongoing signal interference on VHF communications channels from "stations purporting to represent the Chinese military" over the western Pacific Ocean and South China Sea
 - Some flights also experiencing GNSS jamming and radar altimeter (RADALT) interference
 - International Federation of Air Line Pilots' Associations (IFALPA) noted that Chinese warships located in the South China Sea, Philippine Sea, and the Eastern Indian Ocean were placing VHF calls to some passenger flights and military aircraft

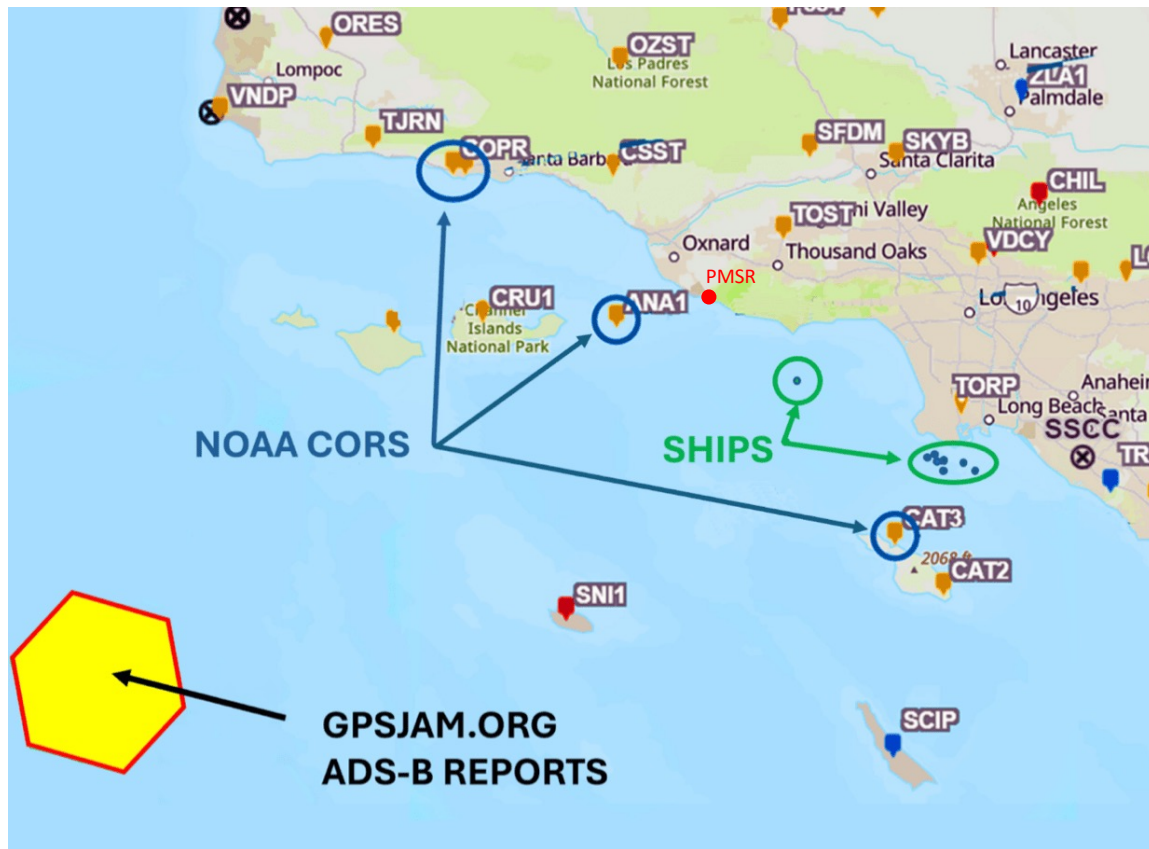


Case Study: GPS Incidents in Aviation (4)

- GPS Jamming at UAV Expo (05/31/2024)
 - Jamming occurred at XPOTENTIAL 2024 conference in San Diego, sponsored by the Association for Uncrewed Vehicle Systems International (AUVSI) and a premier event for UAV operators
 - One of the vendors, NavtechGPS, was able to track the source of the interference to a film crew's wireless microphone, used to interview exhibitors and attendees
 - Because the microphone could not be repaired or replaced, the interference continued intermittently for the duration of the event
 - A 2019 EU project detected more than 450,000 signals that might interfere with GPS and other satnav; >90% were byproducts of mechanical and electrical equipment malfunctions, and unintentional interference



Case Study: GPS Jamming, S. California



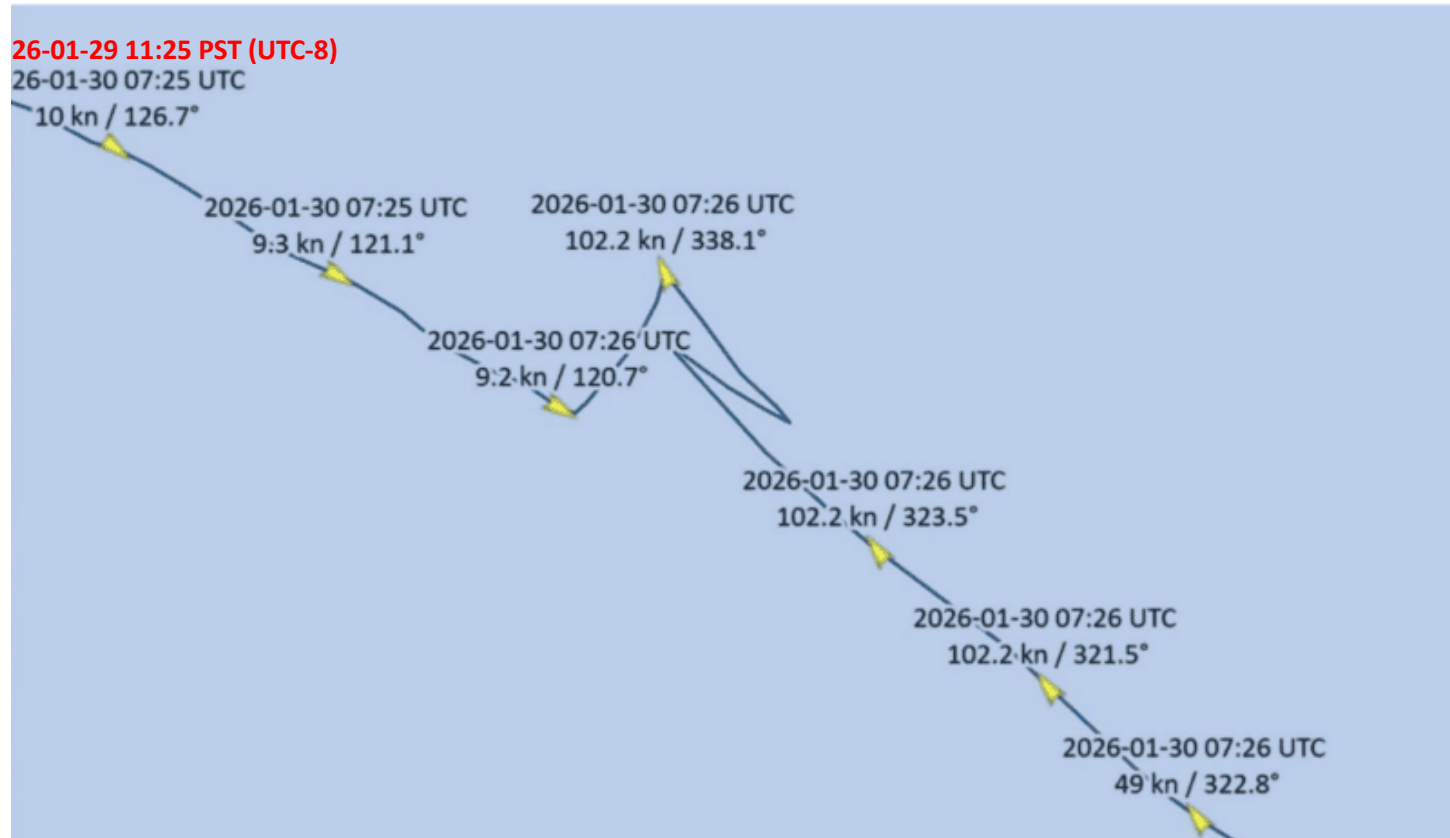
(c) Gary C. Kessler, 2017-2026

Between 2300-0000 on 01/29/2026, seven vessels approaching Port of Long Beach reported GPS outages, several aircraft in the area reported ADS-B issues, and the NOAA Continuously Operating Reference Station (CORS) Network reported anomalies on L1 and L2.

Several vessels' AIS tracks were consistent with GNSS spoofing, and at least one ship lost AIS entirely. Many vessels were operating in close proximity in traffic separation lanes.

Anomalies are believed to be the result of a GPS test at the Naval Air Warfare Center Weapons Division's Point Mugu Sea Range (PMSR).

Case Study: AIS Track of Container Ship



(c) Gary C. Kessler, 2017-2026

Case Study: Seven Cabins Fire

- New Mexico Air Ambulance Crash & Wildfire (05/2026)
 - Beechcraft C90 air ambulance crashed in pitch-black early morning hours in Capitan Mountains near Lincoln, New Mexico
 - Two pilots and two flight nurses killed
 - Impact sparked a destructive wildfire known as the "Seven Cabins Fire," which burned 31,000 acres and lasted 29 days
 - Aircraft's GPS systems were severely disrupted by a nearby U.S. military electronic warfare exercise



(c) Gary C. Kessler, 2017-2026

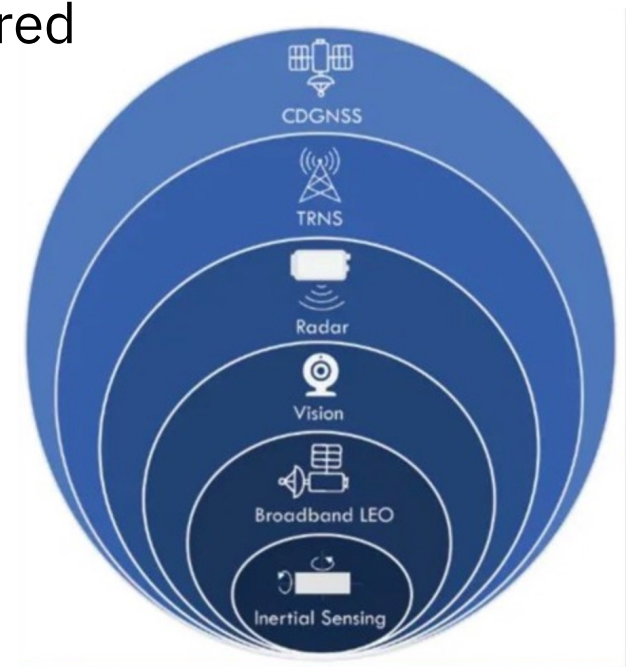
GPS Jamming and Flight Operations

- Flight Management System (FMS) hierarchy for navigation
 - GPS
 - Inertial Reference System (IRS)
 - Employs gyroscopes, accelerometers, and other sensors to determine position
 - Errors accumulate over time
 - DME/DME
 - VOR/DME
 - Distance Measuring Equipment (DME) for slant distance and VHF Omnidirectional Range (VOR) for bearing
 - Dead Reckoning



Case Study: Jam-Resistant Drones

- Critical PNT-dependent systems require layered robustness
 - Carrier-phase-differential GNSS
 - Terrestrial Radio Navigation System
 - Radar
 - Vision
 - Broadband Low Earth Orbit PNT
 - Inertial navigation
- Low-cost anti-jamming chips can make drones GPS-jamming resistant





KANGTAO TDXL-KGR1101 11-element anti-jamming array antenna-4B3+4S+L+B1/L1+GLN

3 sold

\$6,019.32

Wholesale 3+ pieces, extra 45% off

Import charges included ; Extra 5% off with coins

\$29.22 off over \$73.05

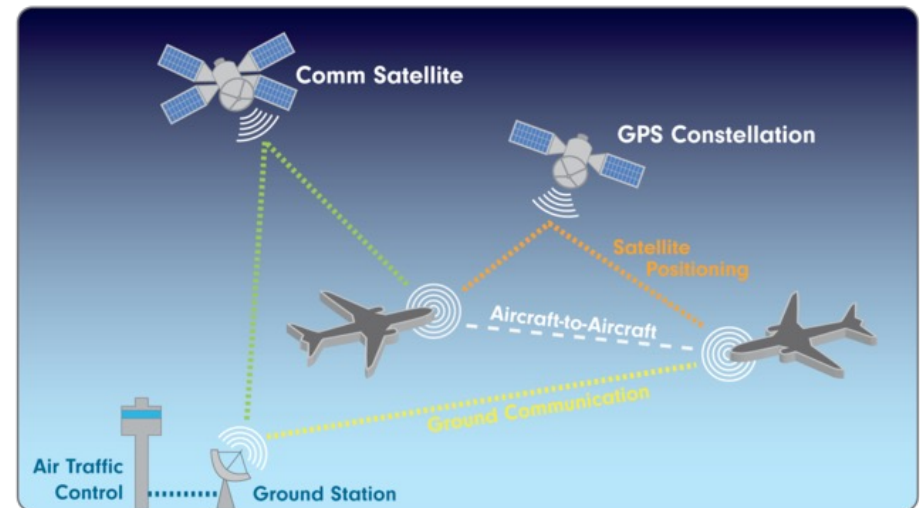
Product sellpoints

- Low-profile design & corrosion resistance:Low-profile design ensures easy integration with terminals, plus corrosion-resistant materials for durability.
- Wide beam pattern & good elevation performance:Offers a wide beam pattern and excellent high/low elevation performance for optimal coverage.
- High unit gain & consistent performance:Boasts high unit gain and consistent performance across all bands for reliable signal reception.
- Kangtiao Tdxi Kgr1101|Kangtiao Tdxi Kgr1101 Antenna|11-element anti-jamming array:Features a robust 11-element array to enhance signal reception and minimize interference.
- BDS 4B3/4S & GLONASS Support:Seamlessly supports BDS 4B3/4S and GLONASS signals for versatile navigation needs.

04/05/2026 (free shipping with delivery by 04/17)

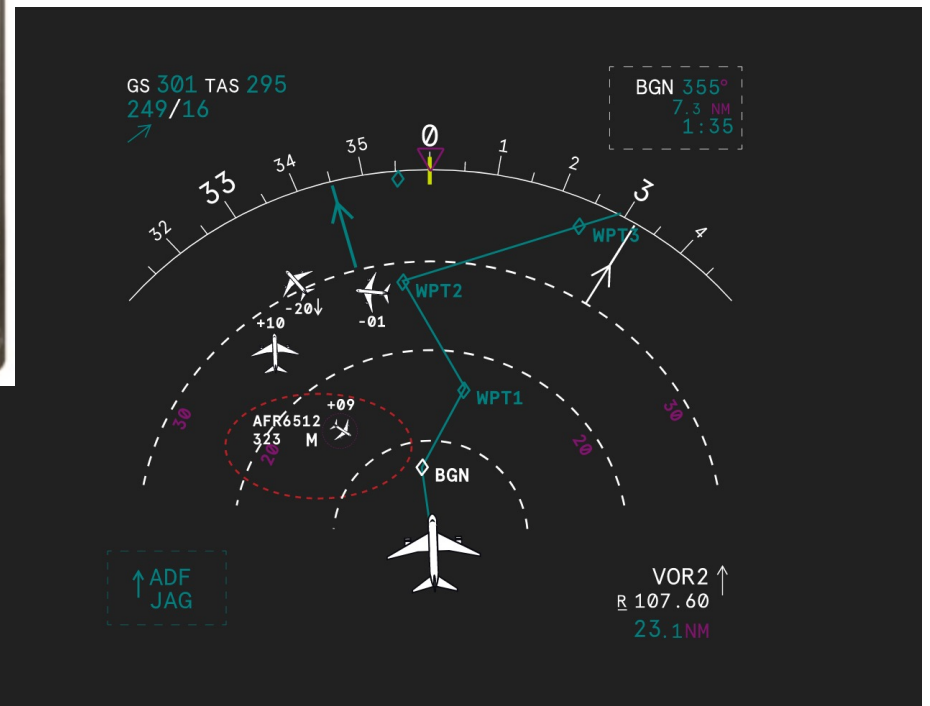
ADS-B

- Automatic Dependent Surveillance – Broadcast
 - Aviation surveillance and situational awareness technology
 - Aircraft obtain position information from GPS constellation
 - Aircraft simultaneously broadcast position ("ADS-B Out") and other data to aircraft and any ground station equipped to receive ("ADS-B In")
 - Ground stations transmit aircraft position information to ATC
 - ADS-B functionality goes down if GPS signal lost





ADS-B Displays



Malaysian Airlines Flight 370

- Malaysian government report (07/2018) suggests that MH370 was "manipulated" off course
 - Boeing 777 was en route from Kuala Lumpur to Beijing with 239 people on board (03/2014)
 - Plane left route, crossed Malaysia, and crashed in the Indian Ocean
 - No evidence of aircraft systems failure nor changes in crew behavior
 - Cockpit data recorders have not been recovered
 - "We are unable to determine with any certainty the reasons that the aircraft diverted from its filed planned route.
The possibility of intervention by a third party cannot be excluded."



Case Study: SAFO 24002

SAFO

Safety Alert for Operators

SAFO 24002

DATE: 01/25/24

- FAA issued SAFO 24002, "Recognizing and Mitigating Global Positioning System (GPS) / Global Navigation Satellite System (GNSS) Disruptions"
 - Inability to use GPS/GNSS for navigation;
 - Inability to use hybrid GPS/GNSS inertial systems for navigation;
 - Loss of area navigation (RNAV) capability, to include required navigation performance (RNP);
 - Unreliable triggering of Terrain Avoidance and Warning systems (TAWS);
 - Inaccurate aircraft position on navigation display (e.g. moving map and electronic flight bag);
 - Loss of or erroneous Automatic Dependent Surveillance-Broadcast (ADS-B) outputs;
 - Unanticipated effects to use of conventional navigation aids (e.g. inability to autotune);
 - Unanticipated position-dependent flight management system effects (e.g. insufficient fuel indication)
 - Failure or degradation of Air Traffic Management (ATM) infrastructure and its associated systems reliant on GPS/GNSS, resulting in potential airspace infringements and/or route deviations.

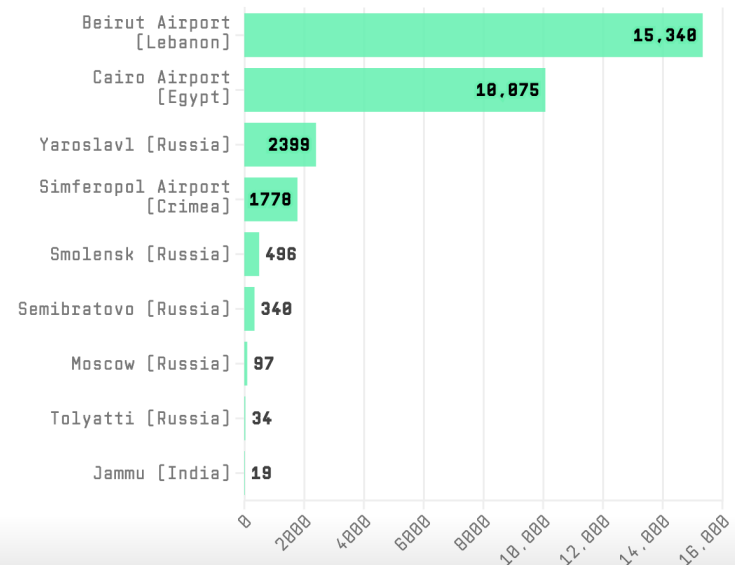
The Prevalence of GPS Spoofing

- The Dangerous Rise of GPS Attacks
(*WIRED*, 04/30/2024)

The attacks can jam signals, essentially forcing them offline, or spoof the signals, making aircraft and ships appear at false locations on maps. Beyond the Baltics, war zone areas around Ukraine and the Middle East have also seen sharp rises in GPS disruptions, including signal blocking meant to disrupt airborne attacks.

Number of Planes Experiencing GPS Spoofing in April 2024

The locations planes appeared to be spoofed to.



Source: GPS Spoofing Map by SkAI Data Services, Zurich University, OpenSky Network

WIRED

Case Study: The End of GPS for Aviation?



(c) Gary C. Kessler, 2017-2026

<https://www.youtube.com/watch?v=wbd9eSw6Gfl&t=1020s>

Case Study: GPS Spoofing And Jamming: Can Civil Aviation Adapt?



(c) Gary C. Kessler, 2017-2026

<https://www.youtube.com/watch?v=Qg2YZU9sqR0&t=18s>

Managing GPS Tampering

- Many airlines are training pilots to recognize and manage GPS tampering (03/2024)
 - Incidents of tampering are particularly prevalent in conflict zones from the Middle East to northern Europe
 - China, Iran, Israel, N. Korea, Russia, and Ukraine are among current offenders
 - Affected aircraft range from small business jets to Boeing 777s
 - Finnair (for example) reports >100 incidents of GPS interference every month (03/2024)
 - GPS disruption can cause inadvertent

Side Note: The Human Element

- NASA report told of incident with airliner captain who refused to believe he could safely fly the ocean without GPS. He also refused to believe that his GPS receiver was being jammed and insisted it had failed.
- It is difficult for people to deviate from their normal patterns of behavior.
- It can also be difficult for people to overcome their pre-conceived ideas, even when others provide information to the contrary.



Part 121 – GPS Navigation

From a Dispatcher's report: *I received a SATCOM call from the Captain, who informed me they were having issues with the left GPS, and it wasn't functioning properly. The aircraft kept going into DME DME Mode, and his Actual Navigation Performance (ANP) value was going up and was currently at 15 miles. [I] explained to them that the area they were in was a known GPS Jamming area (Bulgaria/Romania/Serbia). The Captain did not believe this was the case and continued his explanation...why he thought it wasn't jamming and it was, indeed, the GPS unit going out, even though I told him that this same flight a week ago had GPS jamming happen in the same area. I got aircraft [Technicians] involved, and they stated they couldn't find anything wrong with the GPS. After hearing this, the Captain still wasn't convinced that it was GPS jamming and kept insisting it was a faulty GPS unit. He then proceeded to say he couldn't [fly] the Atlantic crossing with an ANP value of 15 and one GPS unit down. I assured him he could, as I was reading from the circle of entry chart. I told him all that is needed since he was on a random route was VHF, VOR, DME, ADF, and Mode C. He didn't believe me and instructed me to do my research and get back to him before he started the crossing, which was over 2 hours away. He was adamant that if I couldn't provide him with sufficient information on why he can still do the crossing, he was going to divert.... At this point my relief stepped in, and I briefed him on the situation. He said he would research it.*

The crew refused to listen to Dispatch and did not believe Dispatch that they were in a known area for GPS jamming. Train crews to know the signs of GPS jamming and the areas where it happens frequently.

(c) Gary C. Kessler, 2017-2026

Parting Thoughts



(c) Gary C. Kessler, 2017-2026

Some Conclusions

- GPS is most widely used PNT around the world
 - Resilient against nature but not to a direct attack
 - No backup and no global augmentation, particularly for timing services
 - How many of us can use a sextant or LORAN?
- Changes to GPS and other GNSS systems will not fix these problems
 - Even a fix to military applications will not help civilians
- The problems will get worse
 - Military drones show both the need for GNSS and the need to deny GNSS
- The problems will not go away on their own nor go away quickly...