

Primer on GPS RFI and Jamming

Ken Johnston

<https://www.kteqgeospace.com>

ANSLS Oct 5, 2024 White Point, NS



AGRICULTURE
and MINING



POWER GRID



TELECOMMUNICATIONS
CELLULAR and SECURE
COMM NETWORKS



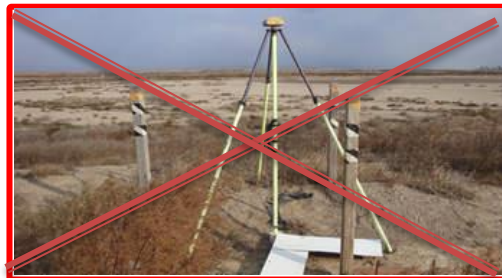
FINANCIAL
SERVICES



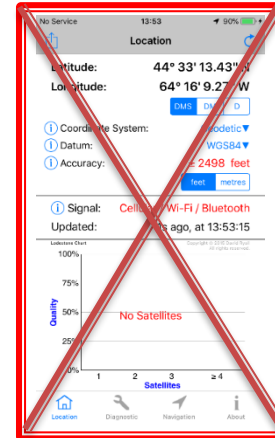
TRANSPORTATION



FEDEX DELIVERY



SURVEY



HAVE QUICK RADIO
TOD

A Day In Your Life Without GPS

00:01 Oct 5, 2024

Positioning, Navigation, **TIMING (PNT)**

FIRST RESULTS – WORLD'S LARGEST JAMMER & SPOOFING TEST BLEIK, ANDOYA, NORWAY SEP 19-23, 2022

*"MANY IMPORTANT AND CRITICAL SOCIETAL FUNCTIONS DEPEND ON
KNOWING THE **EXACT TIME AND PLACE**, AND EXAMPLES OF THIS ARE THE
TRANSPORT SECTOR, POWER SUPPLY, FINANCE, TELECOMMUNICATIONS, AND
SEARCH AND RESCUE"*

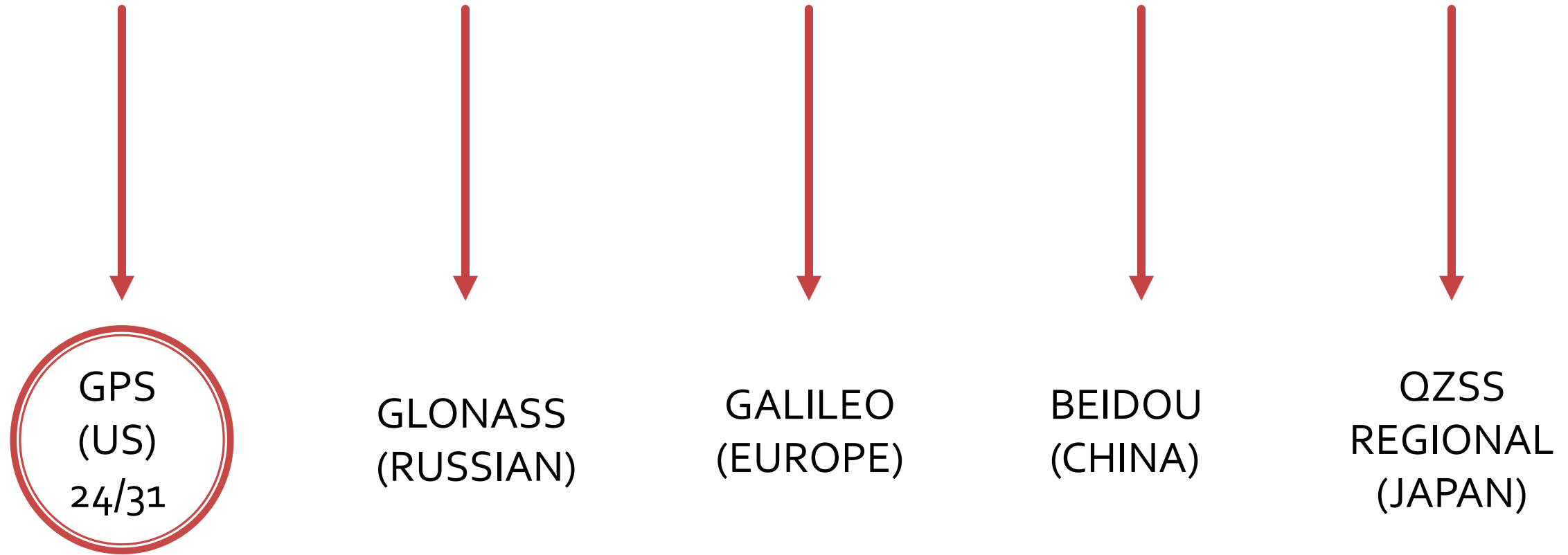


RESILIENT NAVIGATION AND TIMING
FOUNDATION, EDITOR'S BLOG SEP 29, 2022



GLOBAL NAVIGATION SATELLITE SYSTEMS (GNSS)

More than **100** NAVIGATION SATELLITES IN TOTAL



iPhone 12 or newer makes use of some/all these GNSS

LOCKHEED MARTIN

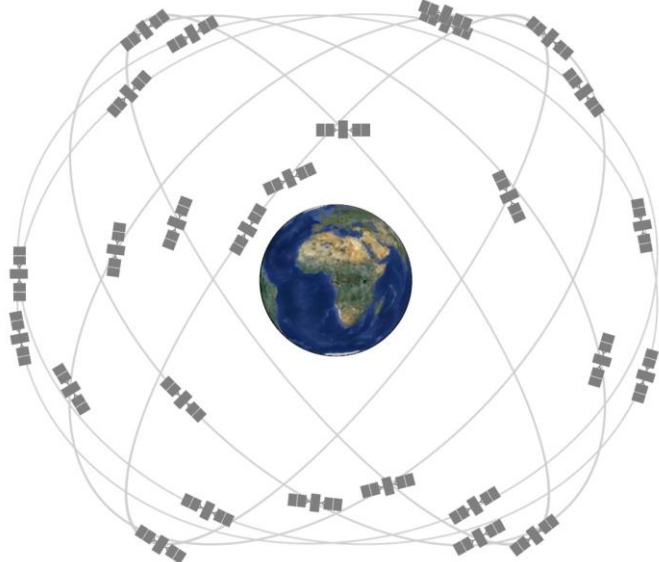
HOME OF GPS III



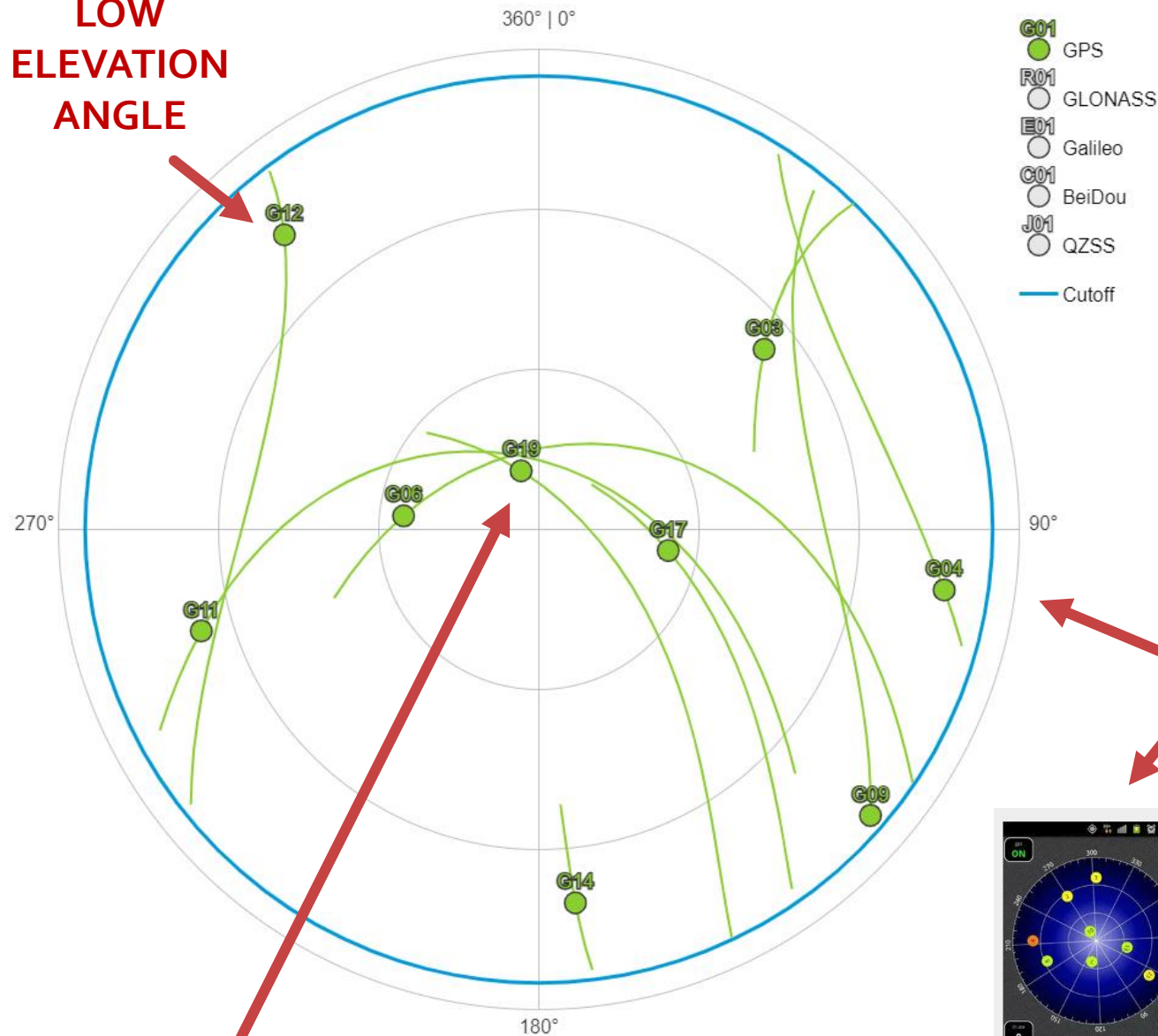
GPS
BLOCK III



GPS CONSTELLATION

- Orbit Altitude of approx 20,184 km (MEO)
 - Orbit Period of approx 12 hrs, 3.874 km/sec
 - Originally six orbit planes with 4 SVs each (24)
 - Each Orbit Plane at 55 degrees inclination
 - Currently 31 SVs – improved accuracy
- 
- **SO WHAT! - design to have at least six satellites in view for a user because need at least four satellites to determine 3D user position & time**
 - Challenges of line of sight to satellite and masking from a building, urban canyon, tree canopy, vehicle, body
 - ANSYS/AGI STK software example and Hula Hoop

LOW
ELEVATION
ANGLE



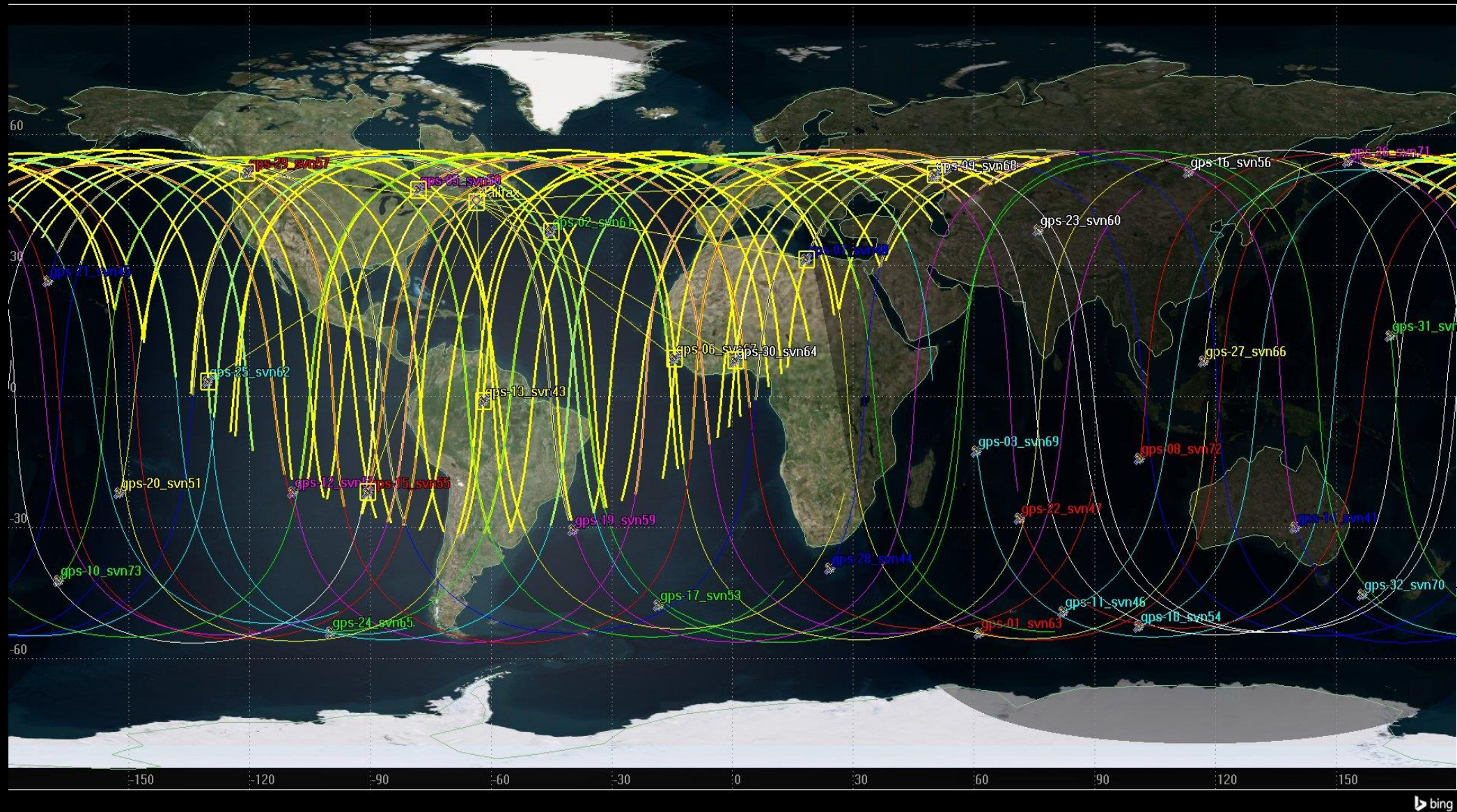
GPS Signal Levels



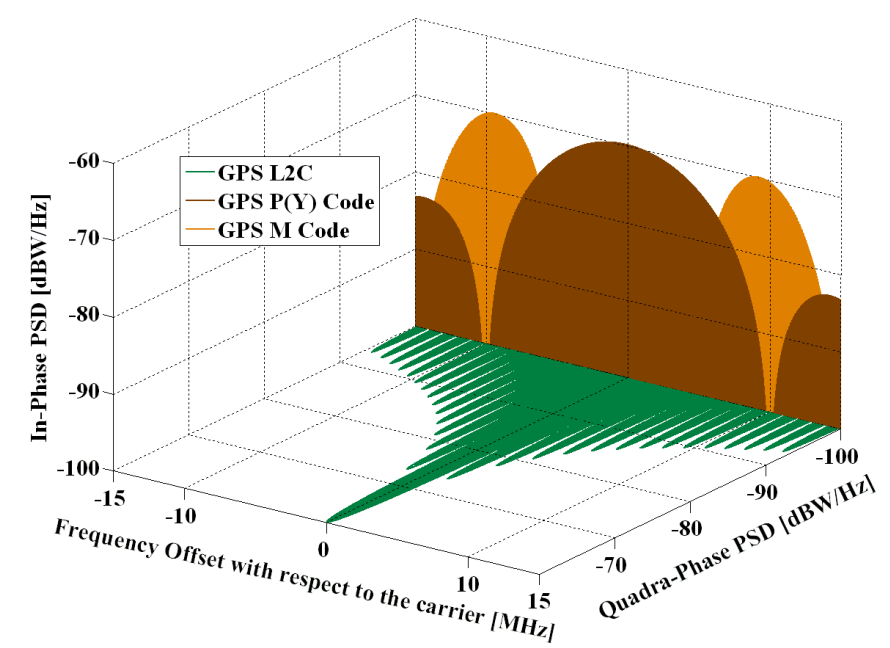
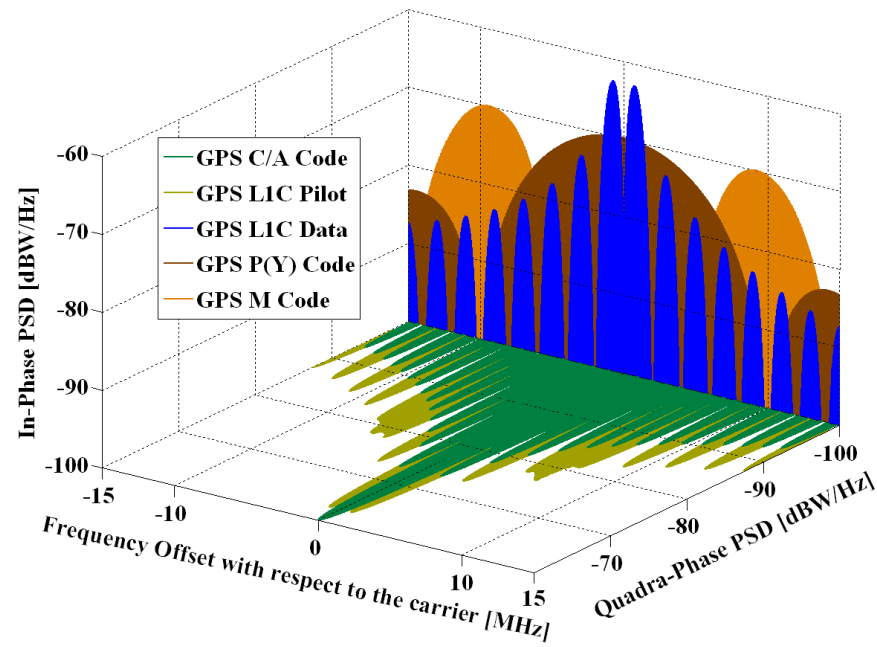
GPS SATELLITE SKY PLOT

HIGH ELEVATION ANGLE





GPS ACCESS PLOT – HALIFAX -24 Hours
Plot generated using ANSYS STK 11.4 software



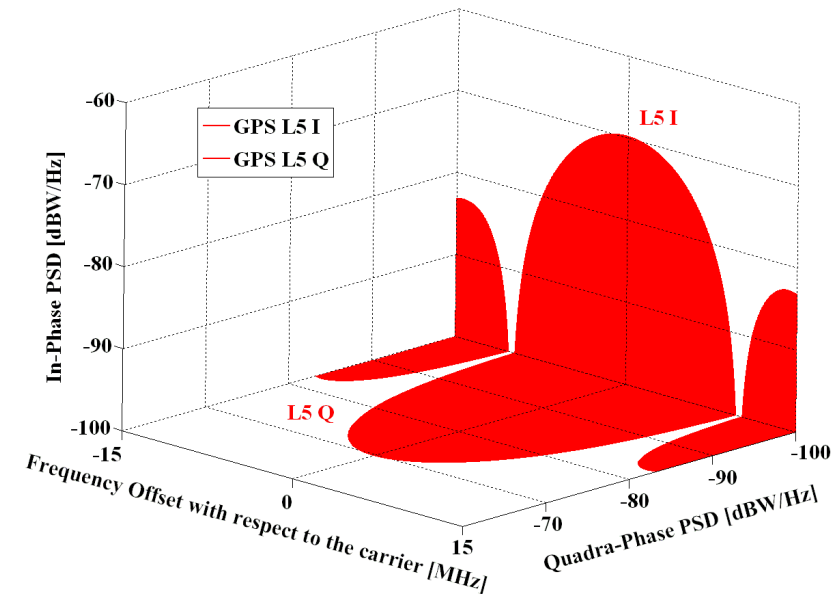
GPS SIGNALS

L1 - 1575.42 MHz

L2- 1227.60 MHz

L5 - 1176.45 MHz

[Lopez - ESA Navipedia]



GPS MEASUREMENT ERRORS

GPS CENTER FREQUENCIES

L1 - 1575.42 MHz

L2 - 1227.6 MHz

L5 - 1176.45 MHz

Measurement Errors

- SA – before May 2000
- ionosphere
- troposphere
- multipath
- clocks / ephemeris
- receiver noise

**DUAL FREQUENCY L1 and L2 / L5
REMOVE IONOSPHERIC ERROR**

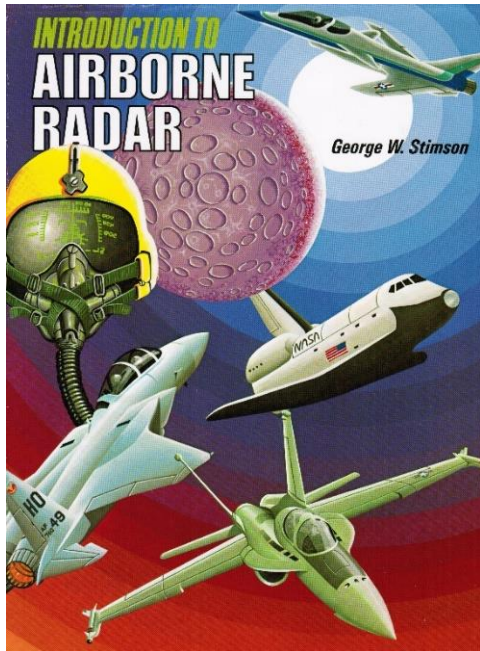
APPLE WATCH ULTRA
and
IPHONE 14PLUS

Dual Frequency
GPS L1 plus GPS L5
capability
(in addition to other
GNSS capability)

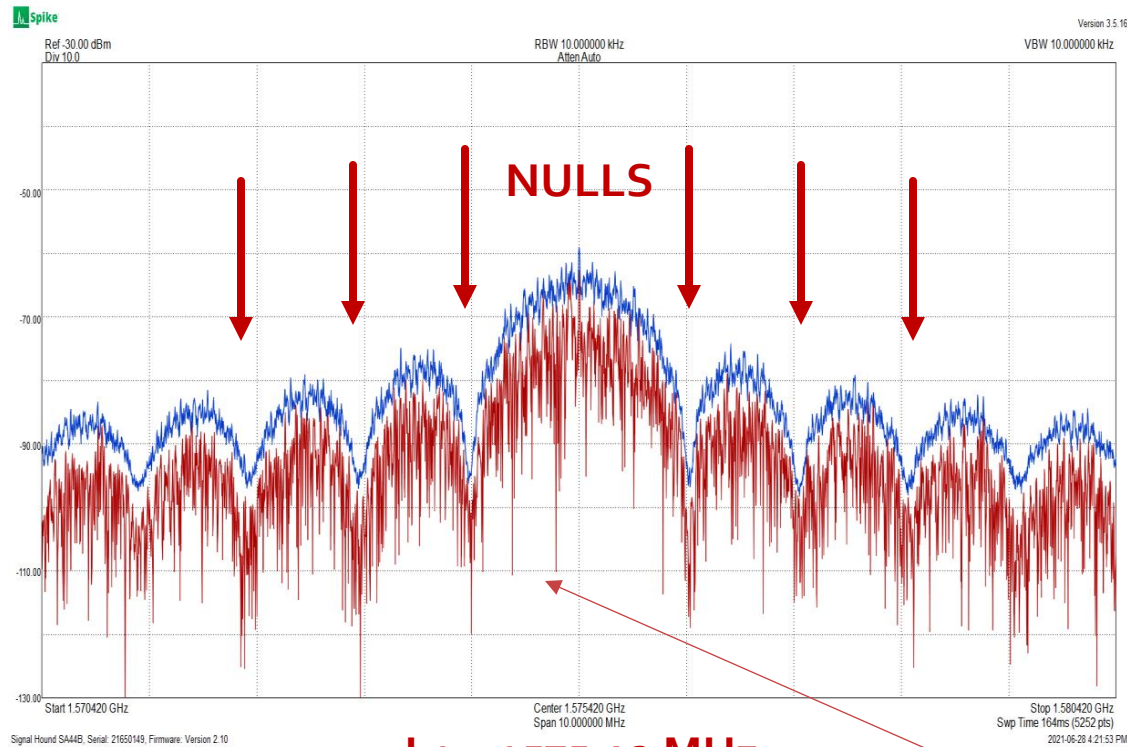


Dual GPS frequency
Removal of Ionospheric Errors
Potential for Better than 1 meter accuracy

L1 C/A chip length of **977.5 ns** sets the Bandwidth Null Spacing of **1.023 MHz** and a central spectral lobe spacing of +/- 1.023 MHz



[Stimson]

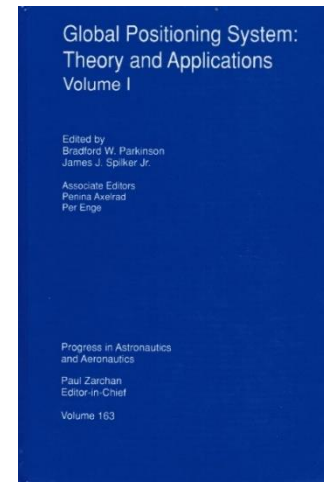
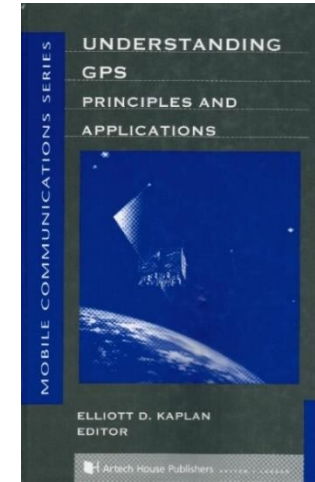


L1 - 1575.42 MHz

$$BW = 1 / PW$$

GPS L2CM	↑	PW	BW	↓
GPS L5	↓	PW	BW	↑

PW and BW and PRF



L1 C/A Code Spectrum [Kaplan/Parkinson]

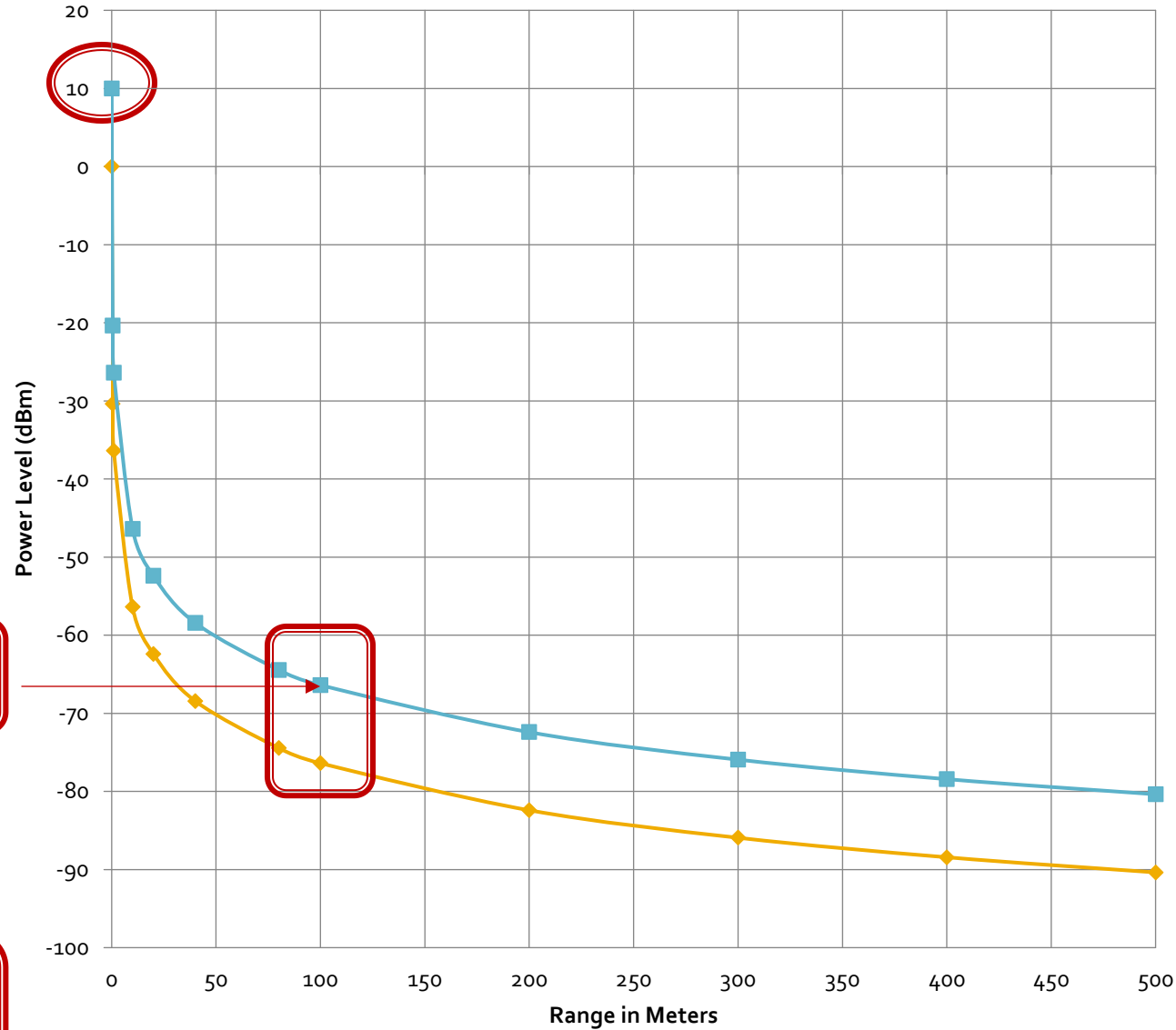
L1 C/A code of 1023 chips has a period of 1 ms sets the spectral line spacing of 1 KHz

Typical output of
RF Sig Gen at 10 dBm



-66 dBm at 100 meters

GPS L1 at
-130 dBm



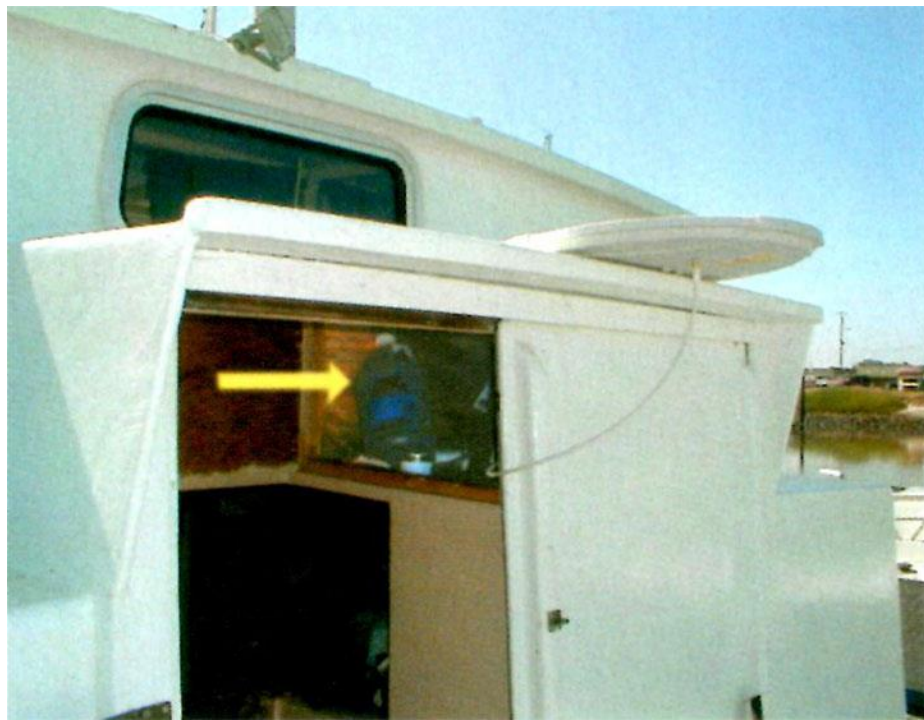
$$\text{Path Loss} = 20 \log \left(\frac{4\pi D}{\lambda} \right)$$

[Richharia]

+10 dBm at 0 meters
-26 dBm at 1 meter
-46 dBm at 10 meters
-66 dBm at 100 meters
-80 dBm at 500 meters
-86 dBm at 1000 meters

-80 dBm at 500 meters

RF Path Loss at GPS L1



UNINTENTIONAL

**GPS RFI
California
2001**

**PPD
Jammer
Testing**

GPS Radio Frequency Interference (RFI)

**Solar Event
March 20, 2023**

**WSMR
Jammer
Testing**



INTENTIONAL



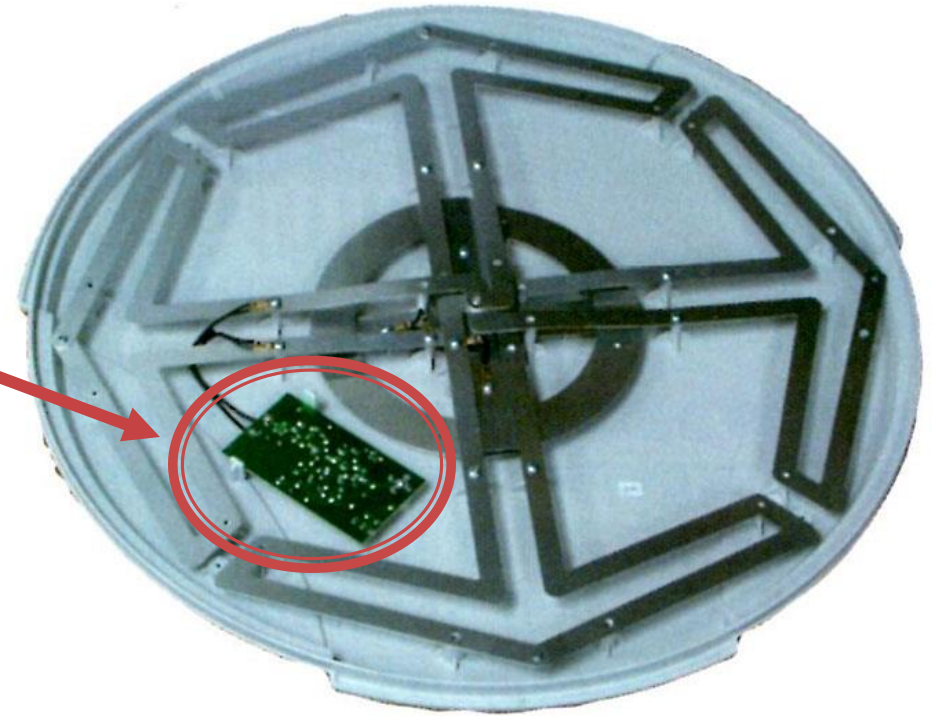
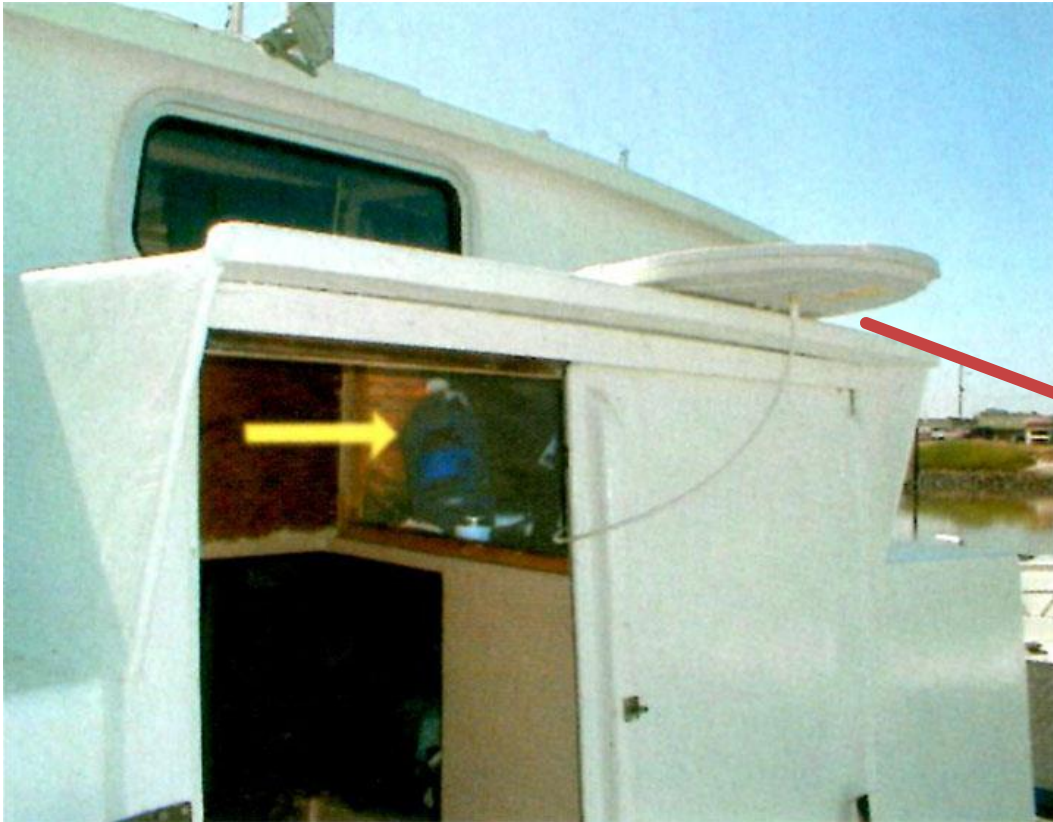
“The Hunt for RFI: Un-jamming a Coastal Harbor”

GPS World Magazine – January 2003



Example of Unintentional GPS Interference Monterey Bay, California – April 2001
MBARI – Monterey Bay Aquarium Research Institute

"The Hunt for RFI: Un-jamming a Coastal Harbor" – Jan 2003



- GPS Radio Frequency Interference (RFI)
- Moss Landing, Monterey Bay, California – April 2001
- Non-intentional RFI – from poor quality TV antenna electronics
- Ref: GPS World - January 2003 <https://www.gpsworld.com/the-hunt-rfi/>



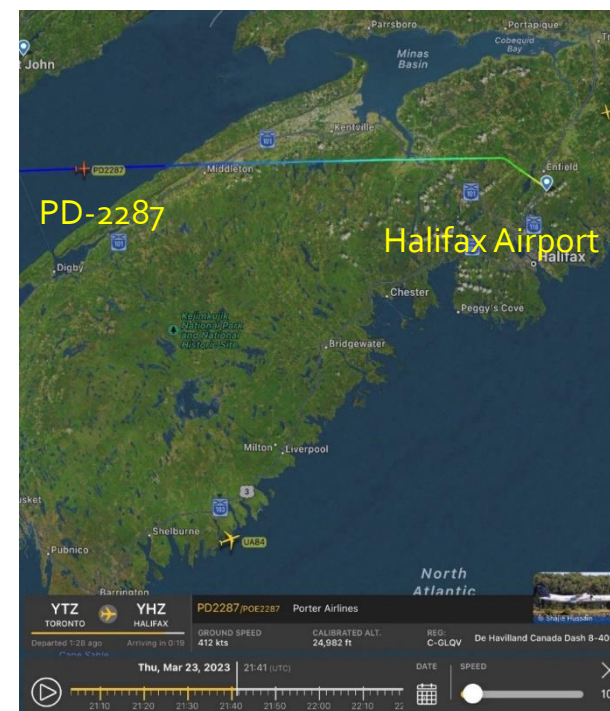
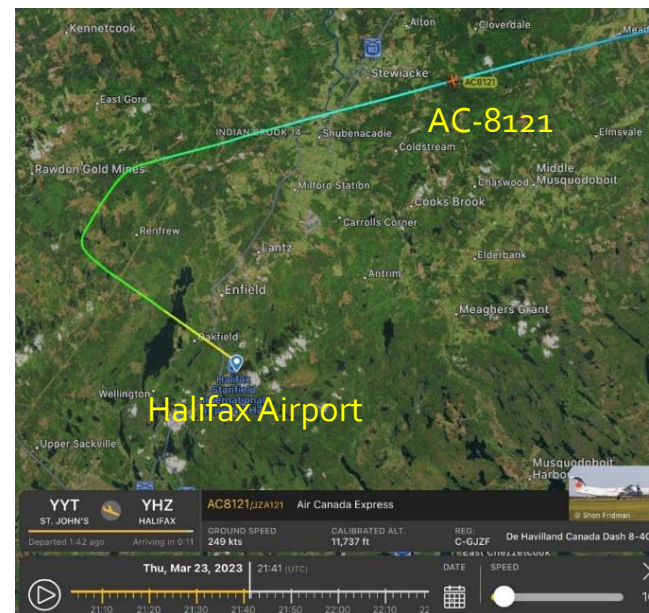
Air Canada C-GJZF

© Shon Fridman



Porter Airlines C-GLQV

© Shajle Hussain



Konstantin von Wedelstaedt

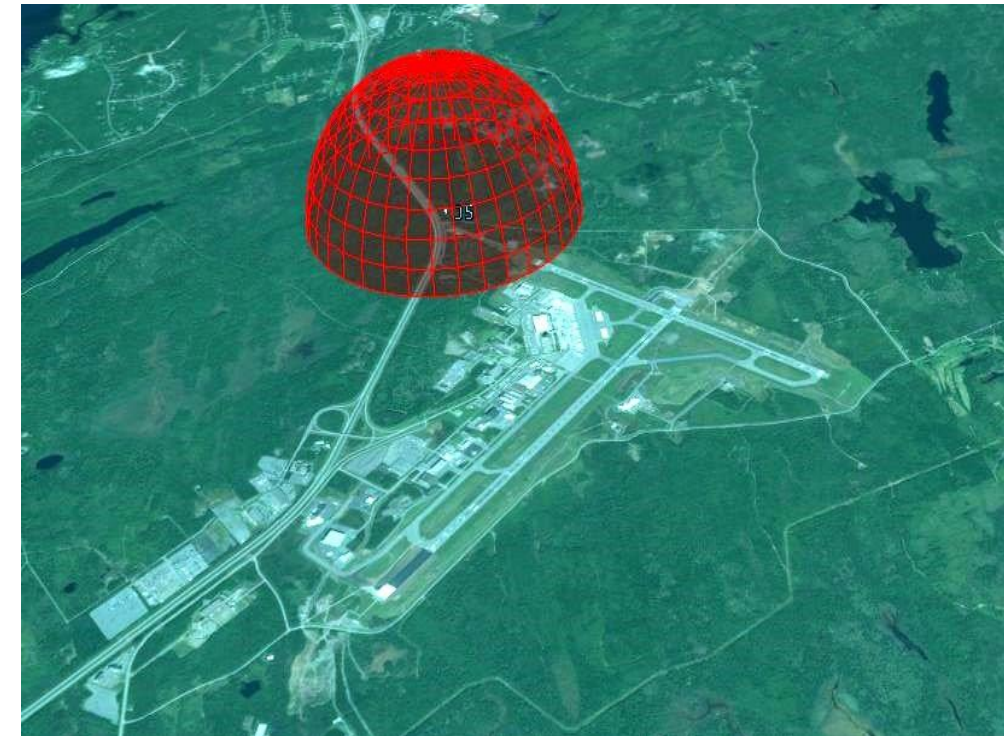
**GPS Signal Anomaly
Reported near
Halifax Airport
(CYHZ) by pilots of
two Dash8 aircraft
on March 23, 2023**

***At the time of the
anomaly both aircraft
were over 180 km apart***

GPS RFI Testing / GPS Jammer / Antenna Masking?

No GPS RFI Reports or NOTAMS of GPS RFI Testing at Halifax Airport

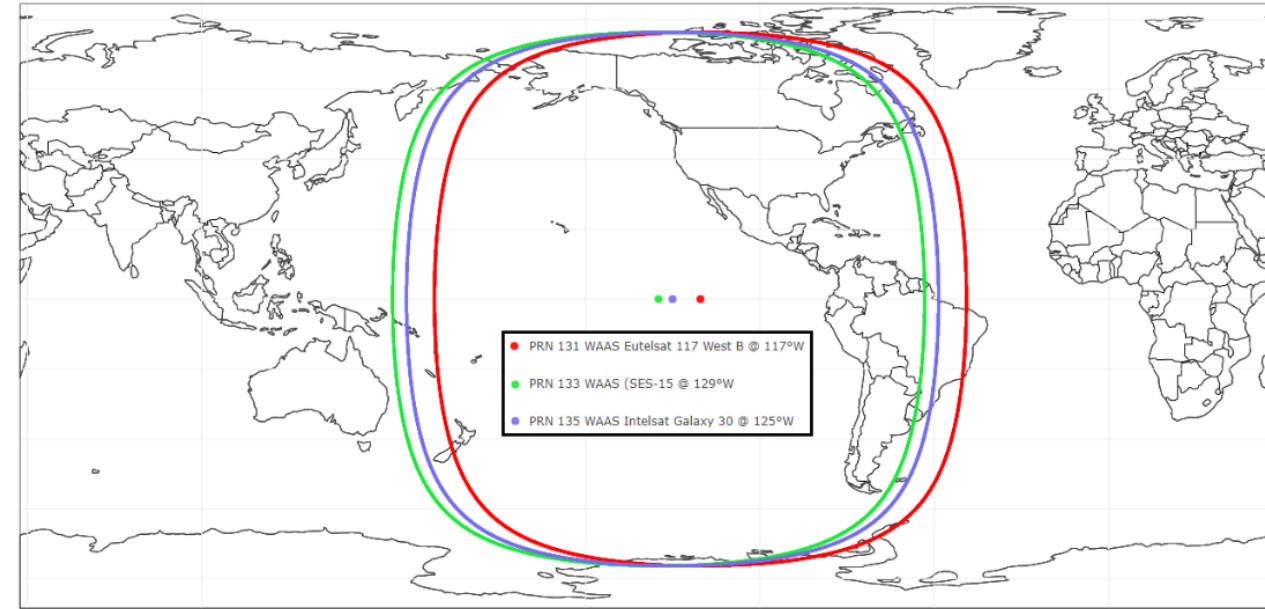
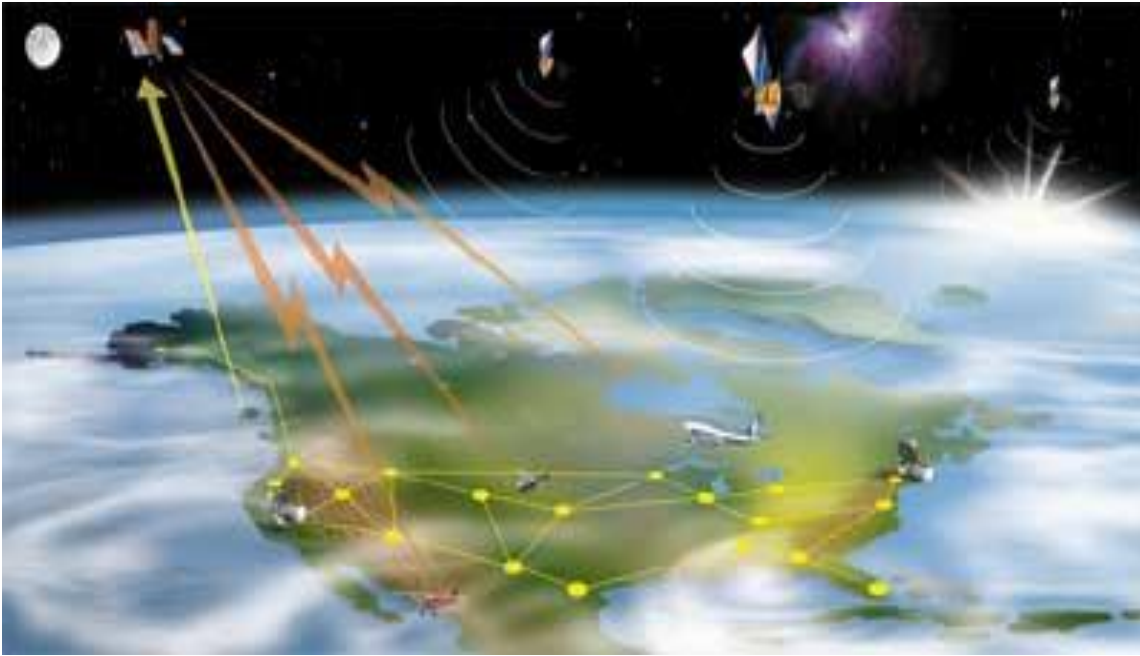
Proximity of Highway 102 to threshold of Runway 14 potential for interference to aircraft from unauthorized use of GPS jammers



SOLAR EVENTS = GEOMAGNETIC STORMS



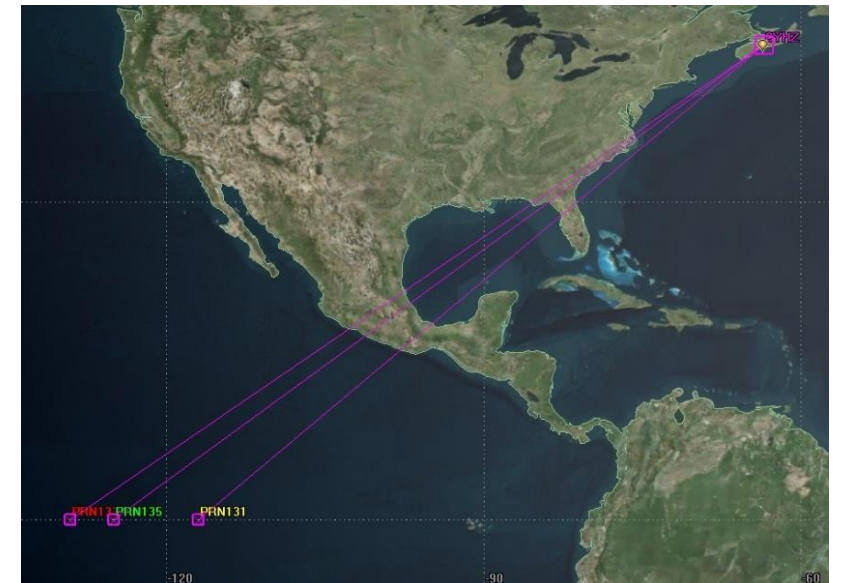
WIDE AREA AUGMENTATION SYSTEM (WAAS)



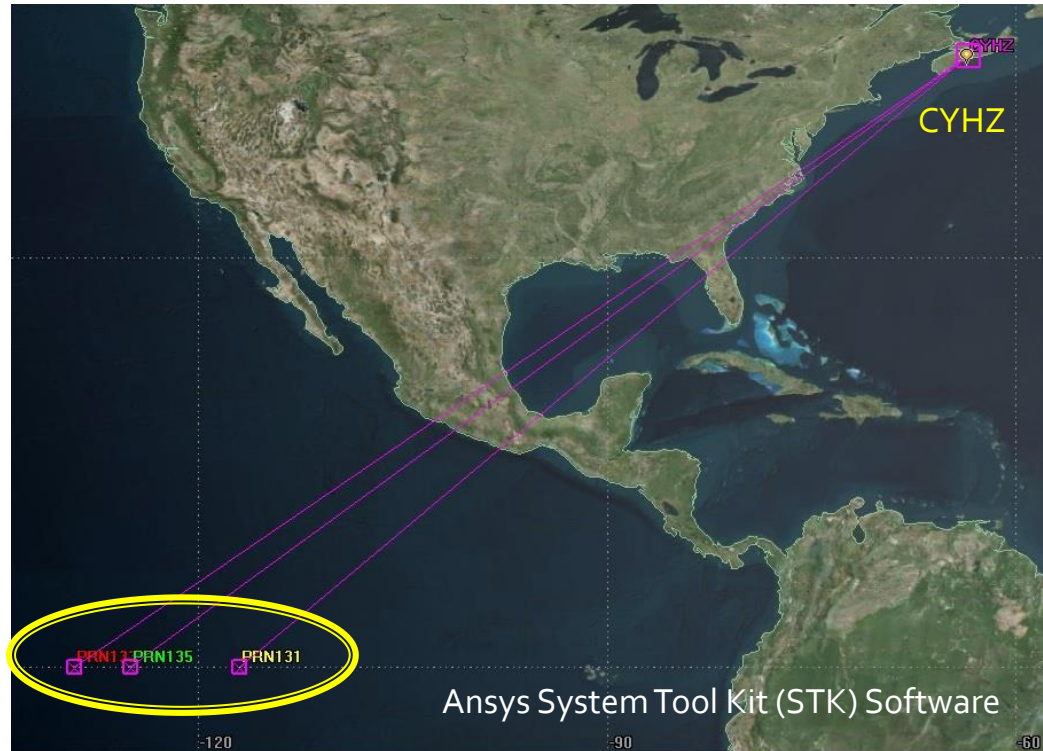
38 ground reference stations in North America

3 WAAS Master Uplink Stations
to three GEO satellites

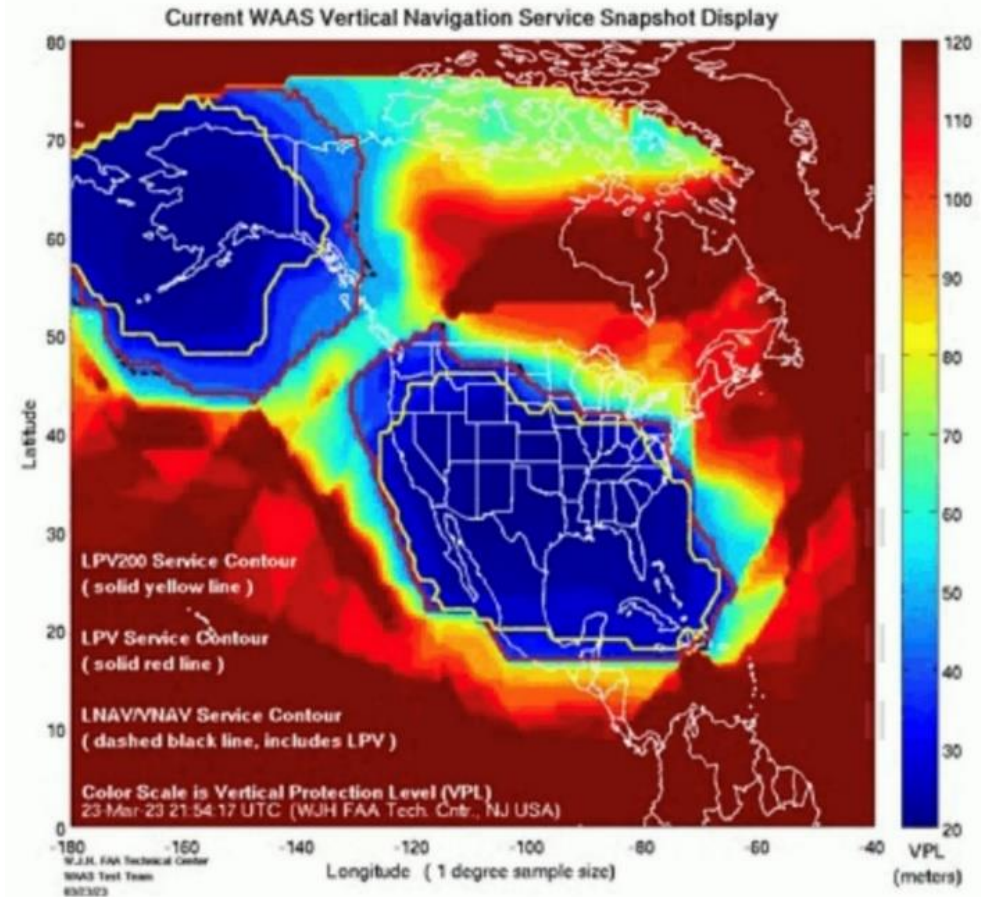
WAAS Corrections sent to GPS users via GEO sats



FAA - Performance Analysis Report #84



PRN 131 (117W) at 242T / 16.6 degrees
PRN 135 (125W) at 249T / 11.2 degrees
PRN 133 (129W) at 252T / 8.4 degrees



WAAS Vertical Nav Service 23 March 2023 at 21:54UTC


WAAS "Significant Degradation" in Canada on March 23/24

<https://kteqgeospace.com/gps-anomaly-research-2023/>

PERSONAL PRIVACY DEVICES (PPDs) – INTENTIONAL JAMMING

jammer-store.com

**GP5000 Car Anti-Tracking GPS
Blocker, Navigation jammer**



Availability: **In Stock**

\$119.99


– 1 +

Buy now

ADVERTISED RANGE – 5 METERS
ACTUAL RANGE – 1 KM

jammer-store.com

**GJ6 Portable All Civil Bands GPS
Jammer, anti tracking device**



Availability: **In Stock**

~~\$459.00~~
\$395.00

– 1 +

Buy now

ADVERTISED RANGE – 20 METERS
ACTUAL RANGE – 5 KM

GPS Jamming/Spoofing is against the law in Canada and the US
Industry Canada – Fines of \$5K-25K / up to 1 year in jail

Why PPD / GPS and Cell Phone Jamming?

To disrupt cell phones and mask a user position from GPS-based tracking systems



Employee vehicle tracking
Rental Cars
Organized crime – drug dealers
Trucker tracking
Prisoner ankle bracelet
Stolen vehicles



Newark Liberty Airport – GPS Landing System Testing

GPS Jamming Incidents 2009-2012

NEWS

N.J. man fined \$32K for illegal GPS device that disrupted Newark airport system

Published: Aug. 08, 2013, 8:28 p.m.



The FCC said an aircraft tracking system at Newark Liberty International Airport experienced interference from a GPS jamming device used by a Readington man who claimed he was simply trying to hide his whereabouts from his employer. The FCC fined the driver \$31,875.

CNET

Tech Money Home Wellness Home Internet Energy Deals Sleep Price Finder More

Join/Login

Culture

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.



Chris Matyszczyk


Aug. 11, 2013 8:08 a.m. PT

2 min read



The company truck that was tracked.


CBS New York Screenshot by Chris Matyszczyk/CNET



15/01/2018

EFFECT OF PPD TYPE JAMMERS ON AVIATION GPS RECEIVERS

Mitch Jevtovic, P.Eng., PMP
Manager, Spectrum Management

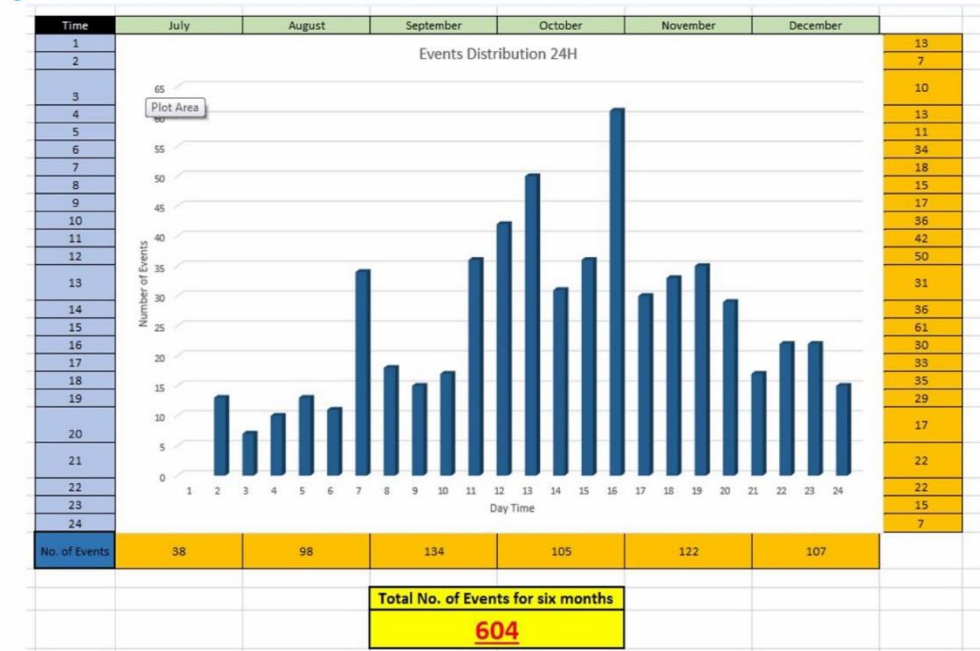


Serving a world in motion
navcanada.ca

Presentation by Mitch Jevtovic, NavCanada
2018 (based on data from 2015-2017)

[https://www.icao.int/NACC/Documents/Meetings/2018/RP
G/RPGITUWRC2019-P17.pdf](https://www.icao.int/NACC/Documents/Meetings/2018/RP
G/RPGITUWRC2019-P17.pdf)

Monthly Events Statistics



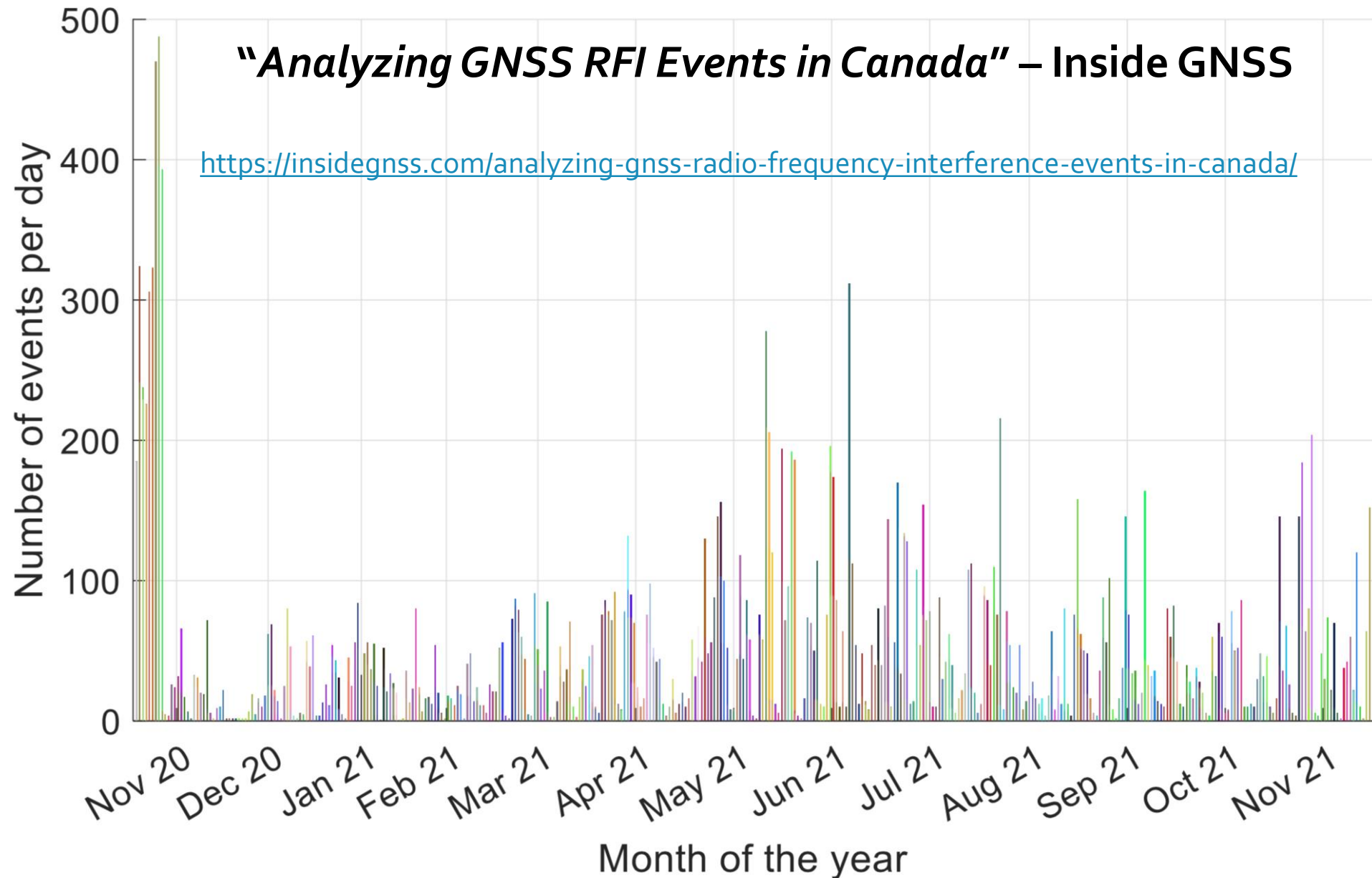
- No significant consequences to airport operation: one complaint from pilot

6 month (July-Dec)
GPS RFI data collection
near Toronto Pearson Airport

604 GPS RFI Events over 6 months

"Analyzing GNSS RFI Events in Canada" – Inside GNSS

<https://insidegnss.com/analyzing-gnss-radio-frequency-interference-events-in-canada/>



GPS RFI Events Nov 2020 – Nov 2021 – Montreal Location – Spirent Detector

York University Canada
and ISED

GPS RFI Events Study

2020-2021

Data Collection for a
location in Vancouver /
Ottawa / Montreal

GPS RFI Event results
research paper for
Montreal site titled,

***"Preliminary analysis
of GNSS radio
frequency interference
events detected in
Canada and impacts
on GNSS-based
applications",***

*Raghuvanshi, A.,
Bisnath, S., Bond, J.*

ION GNSS+

Conference, Sept 2023

Exclusive: Iran hijacked US drone, says Iranian engineer

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.



The Christian Science Monitor - Scott Peterson - 2011

GPS SPOOFING



TED

SIGN IN



How to fool a GPS

819,517 views | Todd Humphreys | TEDxAustin • February 2012

Todd Humphreys – TED Talk – “How to fool a GPS” - 2012

GPSWORLD.COM

August 1, 2012

*"Drone Hack: Spoofing Attack
Demonstration on a Civilian Unmanned
Aerial Vehicle"*

<https://www.gpsworld.com/drone-hack/>



GPS SPOOFING

GPS World article Oct 2017



**James Bond film 1997,
"Tomorrow Never Dies"
GPS signals were spoofed and British
warship lured into Chinese territorial
waters**

**Intentionally misleading a GPS receiver
vs just jamming**

**Excellent explanation of GPS Spoofing and
reported GPS problems by vessels in the
Black Sea reported by ships in June of 2017**

Article from *GPS WORLD* 11 Oct 2017 , Michael Jones, ROKE MANOR RESEARCH
<https://gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>

GNSS Simulators and Repeaters / HackRF One SDR



Spirent GSS7000
GNSS Signal Generator



Spirent GSS6450
GNSS Record and Playback
<https://www.spirent.com>



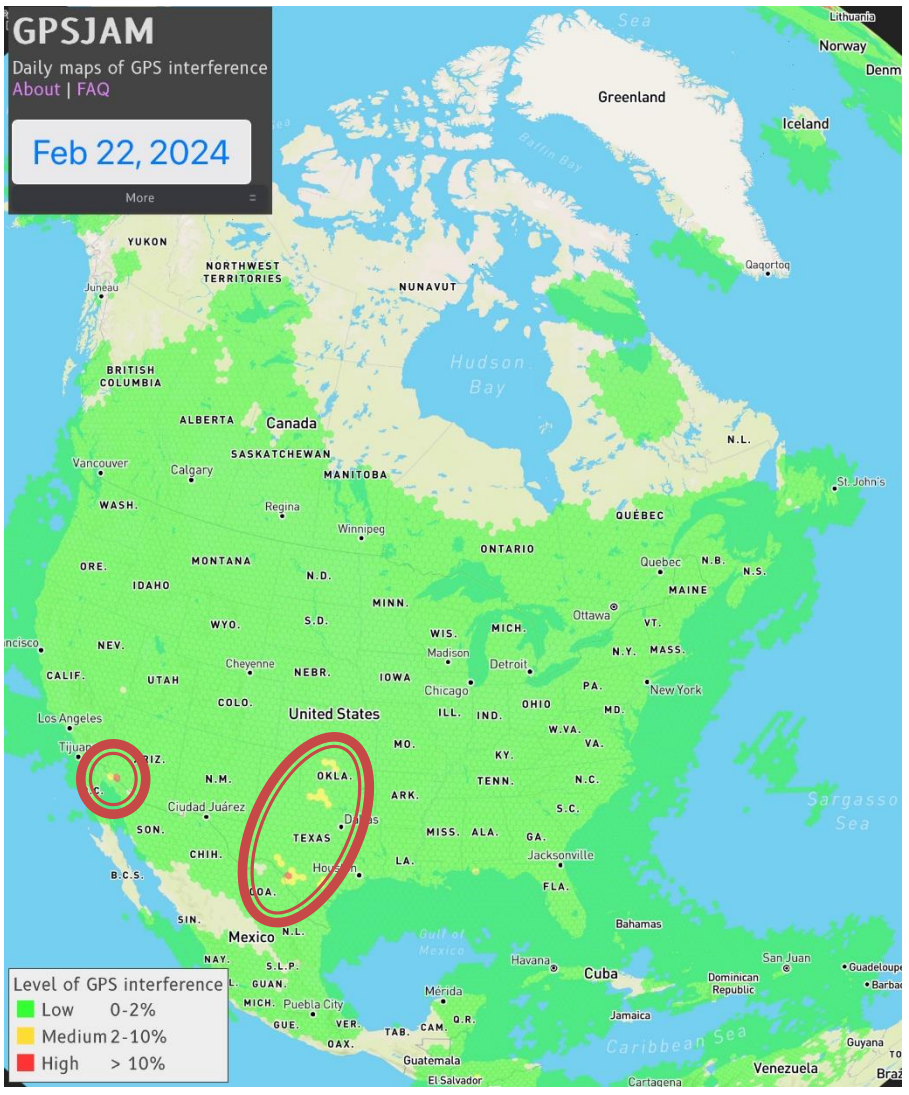
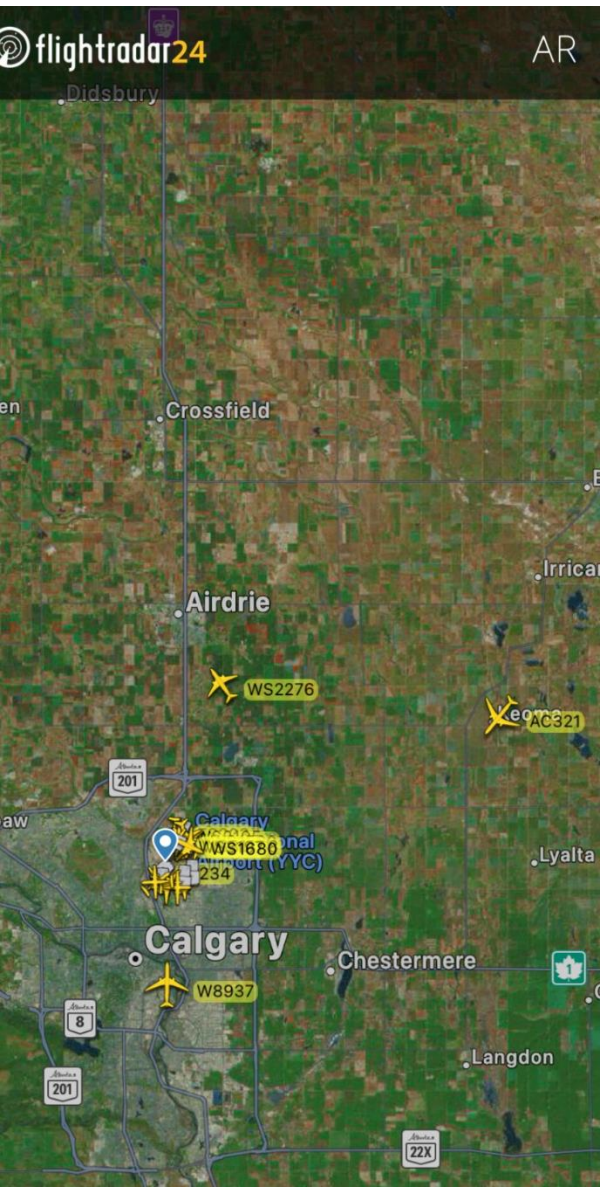
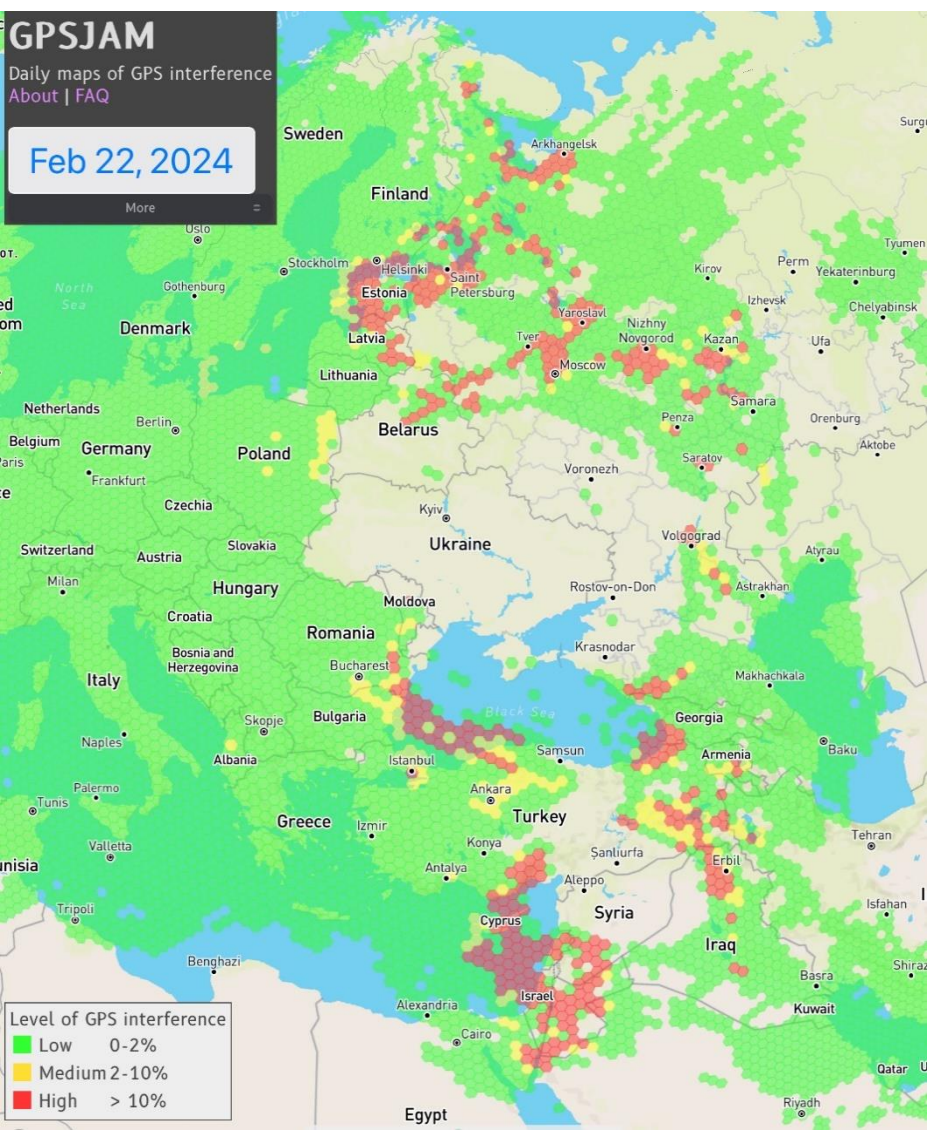
Labsat3
GNSS Simulator/Repeater
<https://www.labsat.co.uk>



HackRF One
Software Defined Radio (SDR)



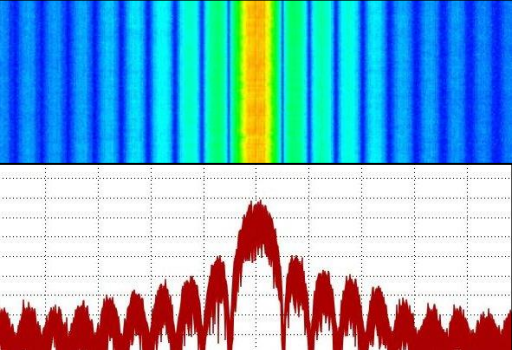
HackRF One SDR + Portapack



<https://gpsjam.org/> website
Daily Map of Global GPS RF Interference
Feb 22, 2024

FlightRadar24 App uses
Aircraft Reported
ADS-B GPS Data

<https://gpsjam.org/> website
Daily Map of Global GPS RF Interference
Feb 22, 2024



Development and Testing of a Low-Cost GPS RFI Emulation System

Canadian Aeronautics and Space Institute (CASI),
ASTRO Conference, Montreal, November 1-3, 2022

KTEQ
GEOSPACE

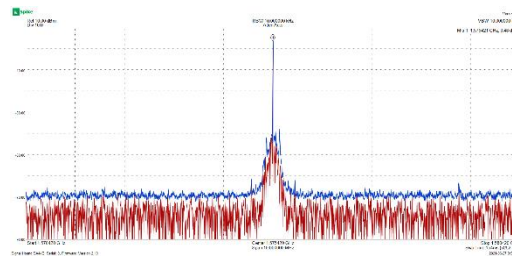


RFI TESTING 1997-99

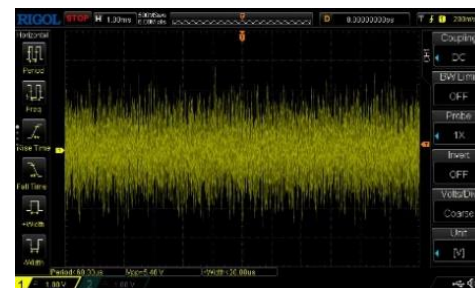
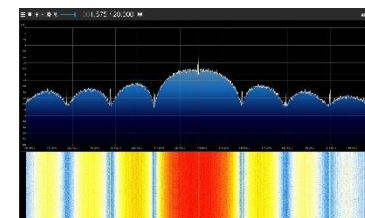


RFI DETECTION 2015

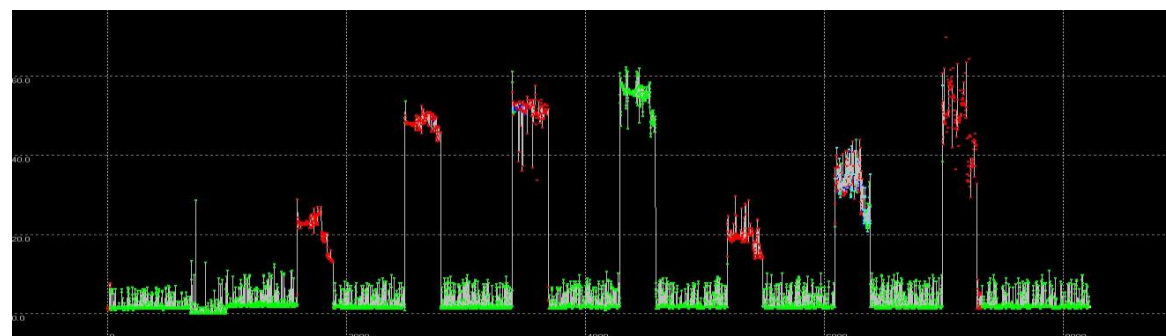
ADF4351



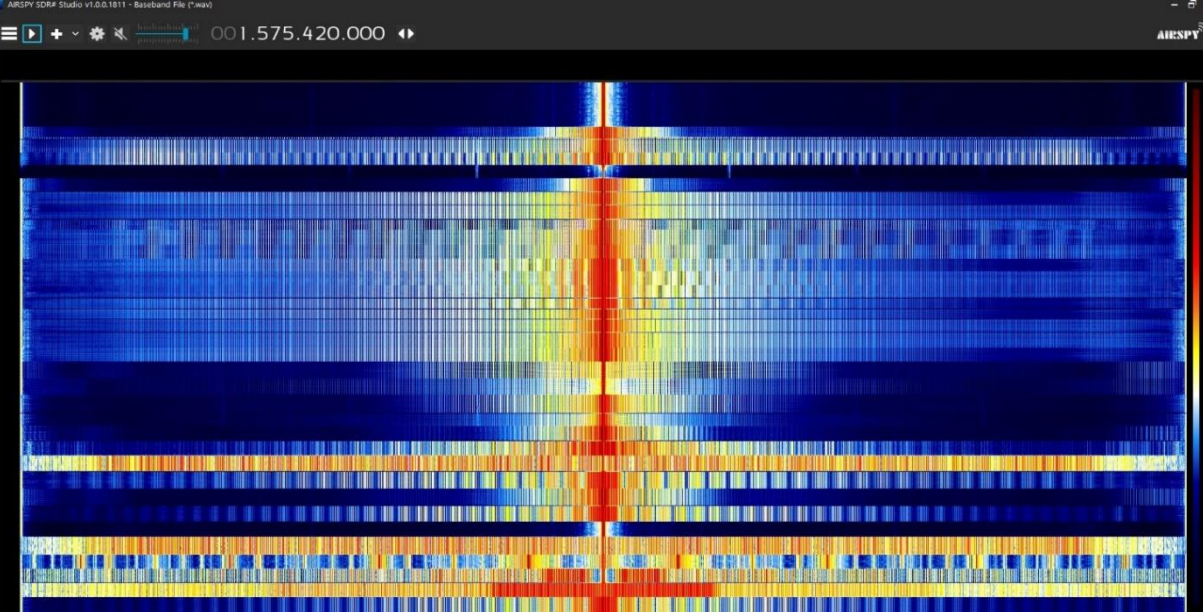
AIRSPY R2 SDR



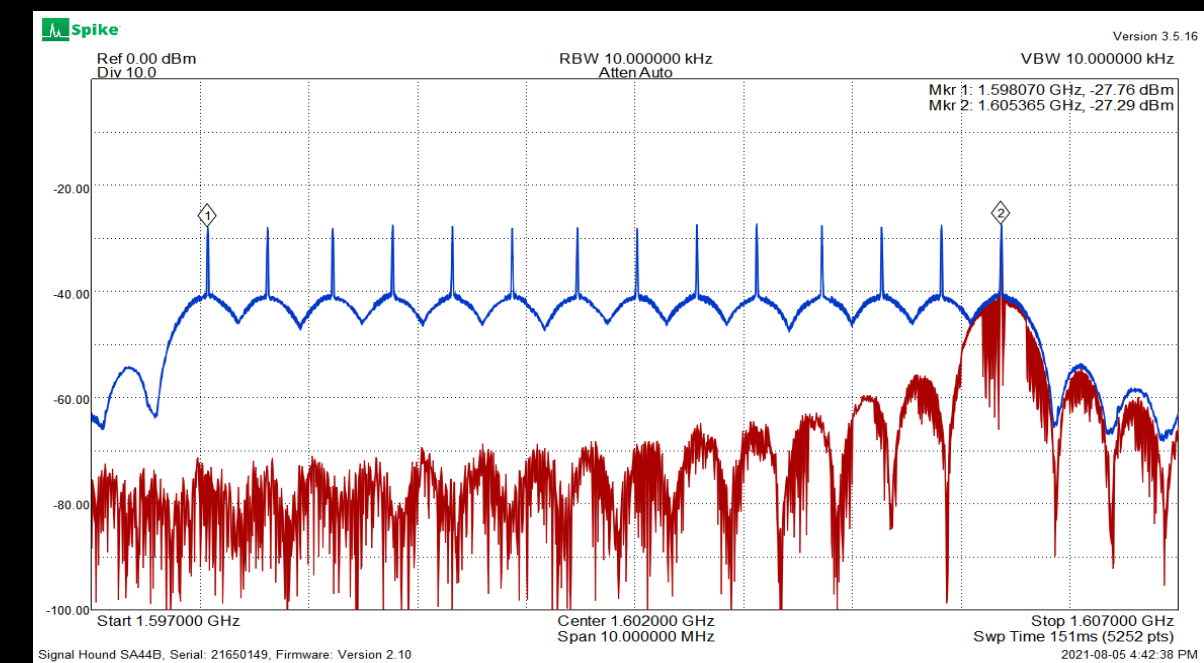
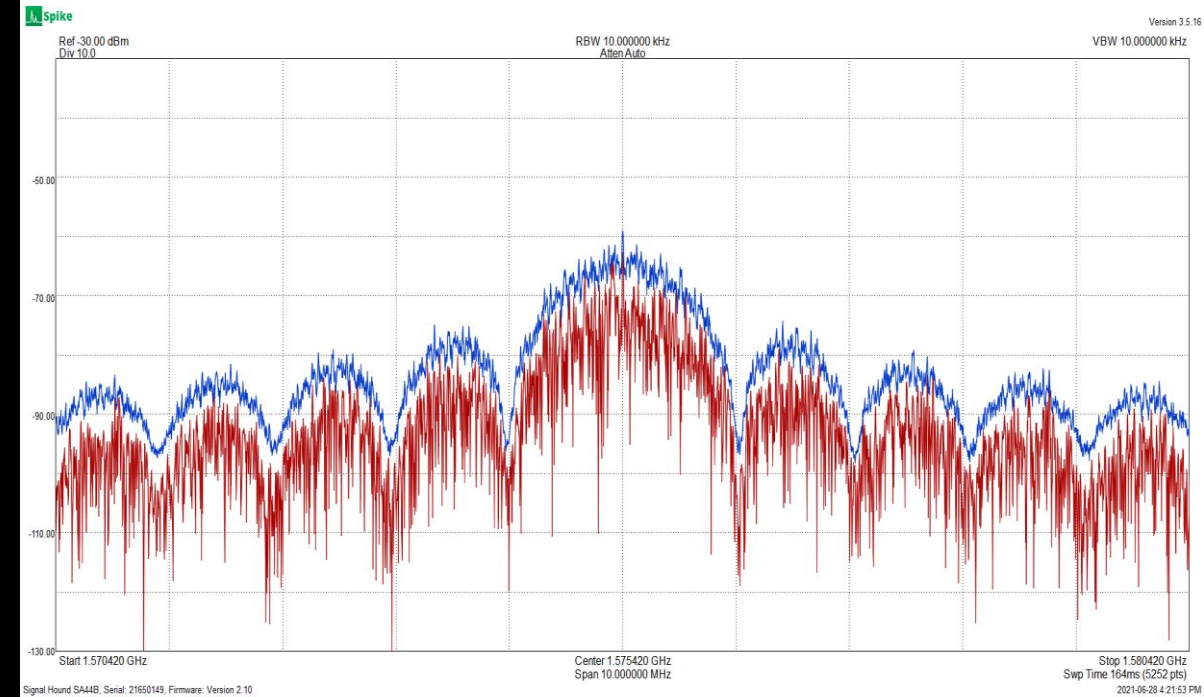
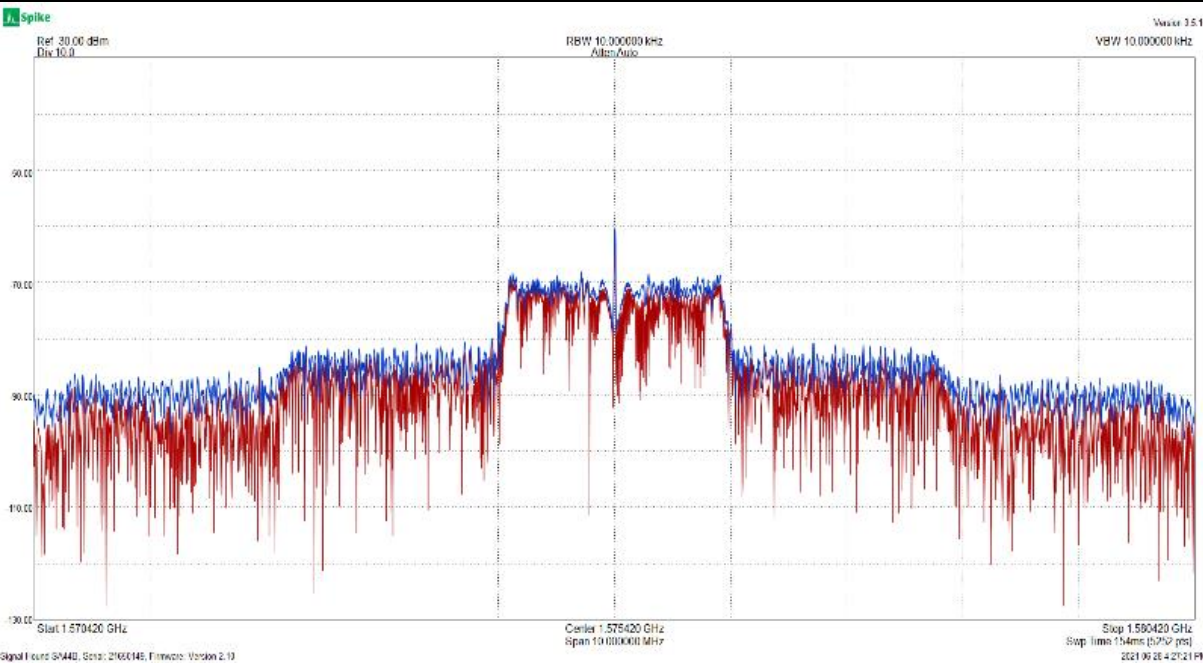
FY6300 AWG

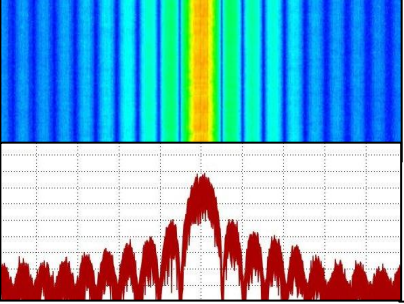


Ublox NEO-7N



GPS / Glonass RFI Emulation - CASI 2022





GPS Spoofing - HackRF One / Portapack H2 Software Defined Radio (SDR)

KTEQ
GEOSPACE

- HackRF One – falls under FCC definition of “Test Equipment”
- By Michael Ossmann
- Great Scott Gadgets
- 2014 Vintage



- Open Source Design
- 20 MHz Bandwidth
- Frequency Range - 1 MHz – 6 GHz
- **Rx – Record - Tx - Half Duplex Transceiver**
- Power Levels – up to 10 dBm at GPS L1
- 8 bit I and Q
- Software Configurable / Linux
- Also works with SDR# Software
- Gqrx/Gnu Radio Companion/**GPS-SDR-Sim**
- Original from Great Scott Gadgets - \$320 USD
- Ebay HackRF One Clones - \$100-130 USD
- Ebay HackRF One + Portapack - \$130-160 USD



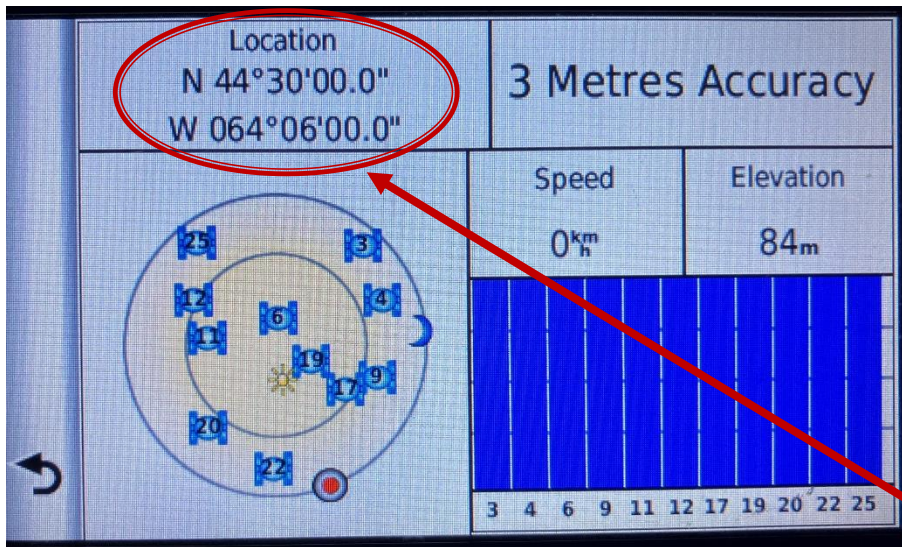
**“Radio Hacking: Cars, Hardware,
and More!”**

Samy Kamkar – AppSec California 2016
Youtube

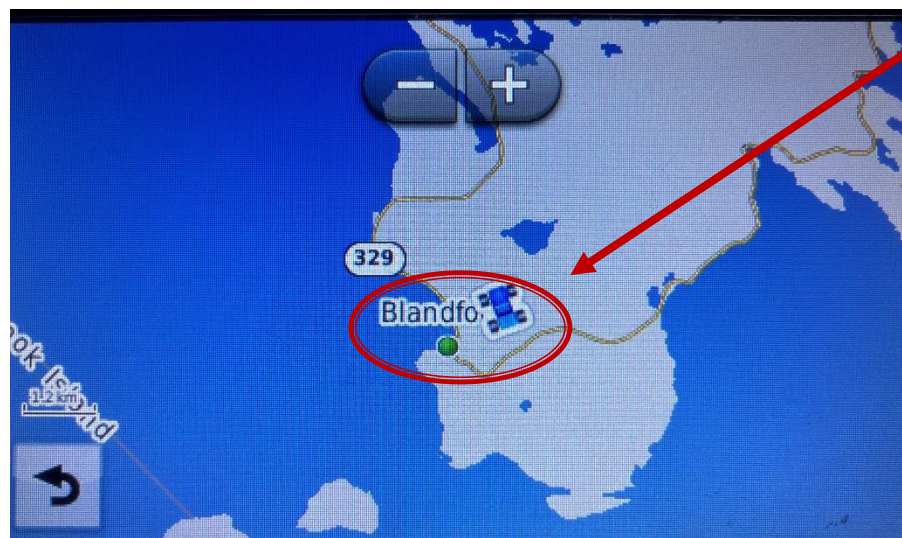
“GPS Spoofing with HackRF on Windows”
TECH MINDS - Youtube

“GPS Spoofer with HackRF One
and Android Phone – Shockingly easy!”
GPSPATRON - Youtube



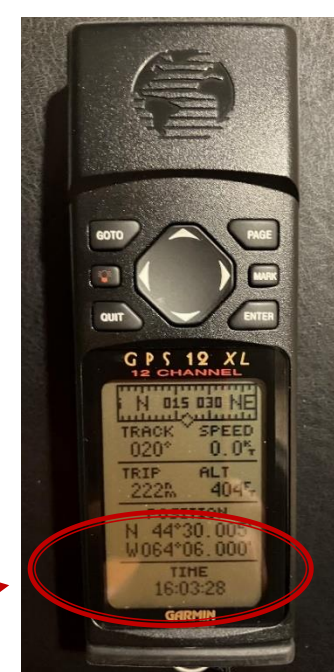


Garmin Nuvi



Note: Signal
Strength Levels
All at Max Value

Garmin Etrex



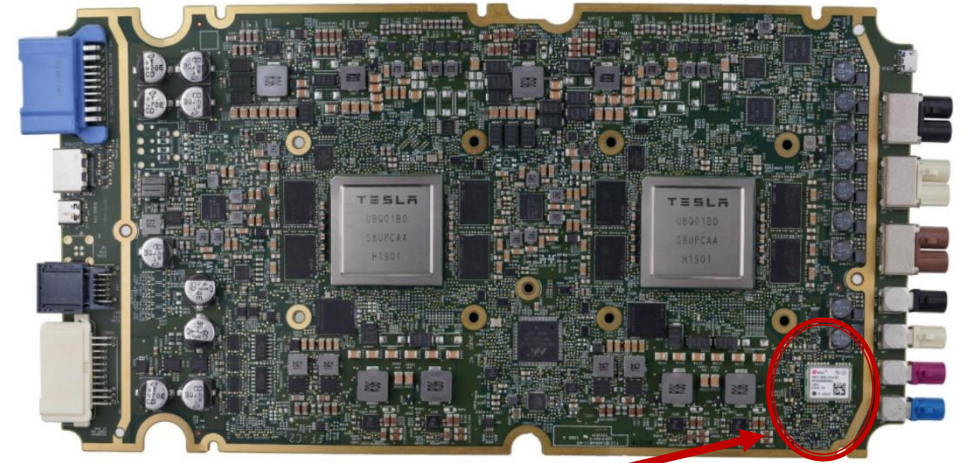
Garmin 12XL

GPS SPOOFING
GPS Position
N44.5 W64.1
Near Blandford, NS
Using
HACKRF One / Portapack
June 13, 2024



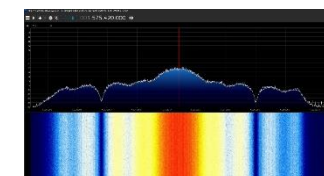
Samsung
Galaxy Cell







**Copy of UBX
file available
for replay in
U-Center
(Look at
SV C/N0,
Noise,
JamInd,
AGC0**



SDR#

**HackRF
One &
Portapack
Spoofing**

**True Date /
Position
(Aug 19, 2024)**

JAMMING

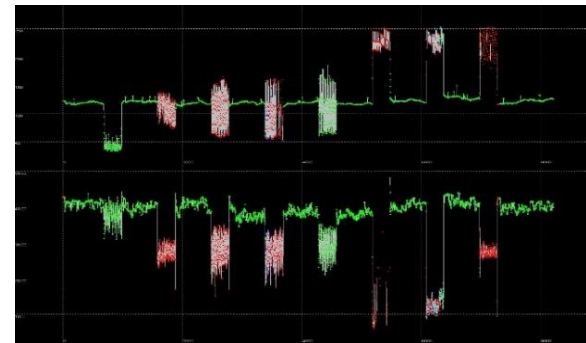
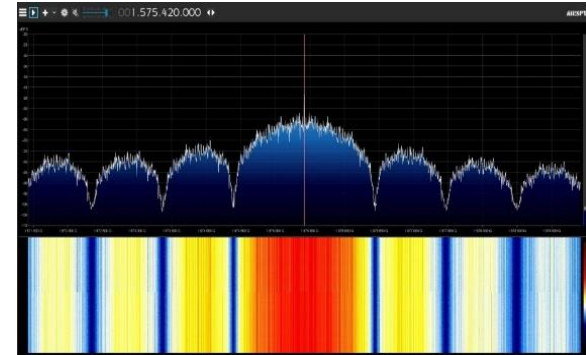
**JAMMING
Spoofed UBlox NEO-M9N
N44.5 W64.1 Spoofed Date: June 13, 2024**

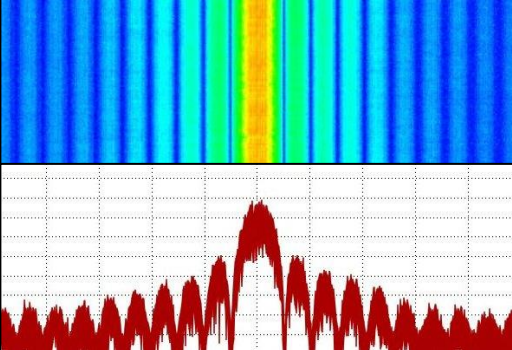
Summary

GPS RFI, Jamming and Spoofing Examples

***Low-cost emulation of GPS RFI
for research, testing,
training and education***

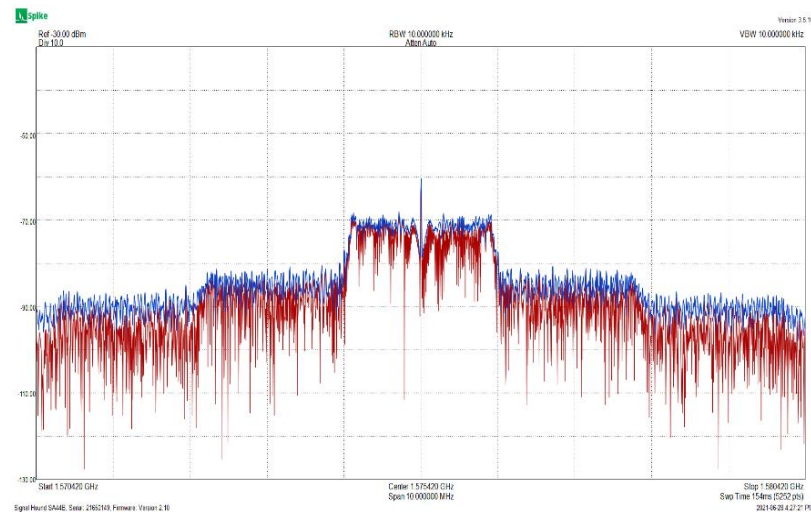
***GPS RFI Detection – Cellphone
GPS Receiver(Ublox) / SDR /
Chronos Handheld RFI
Detectors***





QUESTIONS / FEEDBACK

KTEQ GEOSPACE

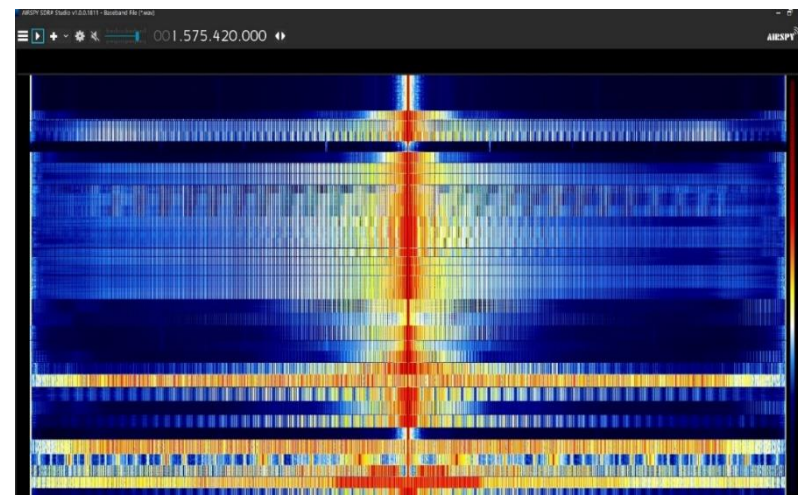
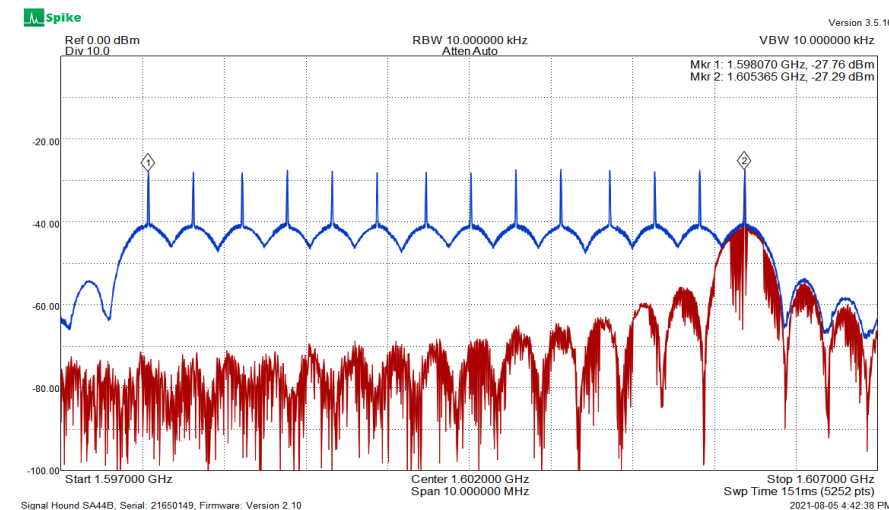


kteqgeospace@gmail.com

<https://www.kteqgeospace.com>

**Ref Papers Presented at:
ION ITM 2022 / CASI ASTRO 2022**

**Google Search
"GPS RFI EMULATION"**



K. Johnston, *Development and Testing of a Low-Cost GPS RFI Emulation System*, Canadian Aeronautics and Space Institute (CASI), ASTRO Conference, Montreal, November 1-3, 2022: https://casi.ca/resources/Documents/ASTRO/2022/Presentations/5B-01%20JohnstonKD_GPS_RFI_Emulation_Paper.pdf

Recommended refs/# from my CASI Paper, KTEQ GEOSPACE website, or Institute of Navigation. <https://www.ion.org/>

[1] Jevtovic

[7,8] Johnston

[24] Grabowski

[25, 56, 57, 58] Mitch et al

[26] Towlson et al

[45] Murrian/Humphreys

[59] Potter et al

<https://www.airspy.com> (SDR# software)

<https://Signalhound.com> (Spike Software)

<https://www.u-blox.com/en/product/u-center>

Further Reading



BACK UP SLIDES



