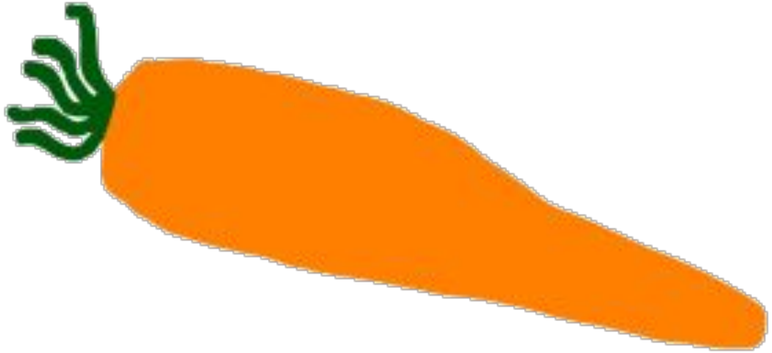


Navigating Planes in a Hostile Radio World

CrikeyCon March 2025

David Robinson/Karit

$ whoami

- David Robinson
- Karit
- Do Security in Wellington
- Kākācon

Today

- How Aviation Navigates
- Attacks on the Aviation Navigation
  - Pilots’ Perspective
  - Air Traffic Control’s Perspective
- What can we do about it?

Terminology

- GNSS - Global Navigation Satellite System
- GPS - Global Positioning System
- If I say GPS generally I will be referring to all GNSS
- GPS, GLONASS, Beidou, Galileo <- World Wide

Where are the planes?

Way back when

- Dead Reckoning
  - Velocity & Time
- Radio
  - ADF, VOR, LORAN

Moved away from them

- Dead Reckoning
  - Hard to factor in wind
- Radio
  - Costly to run
  - VOR still in use but nothing new and decommission to save money
  - Ocean Coverage

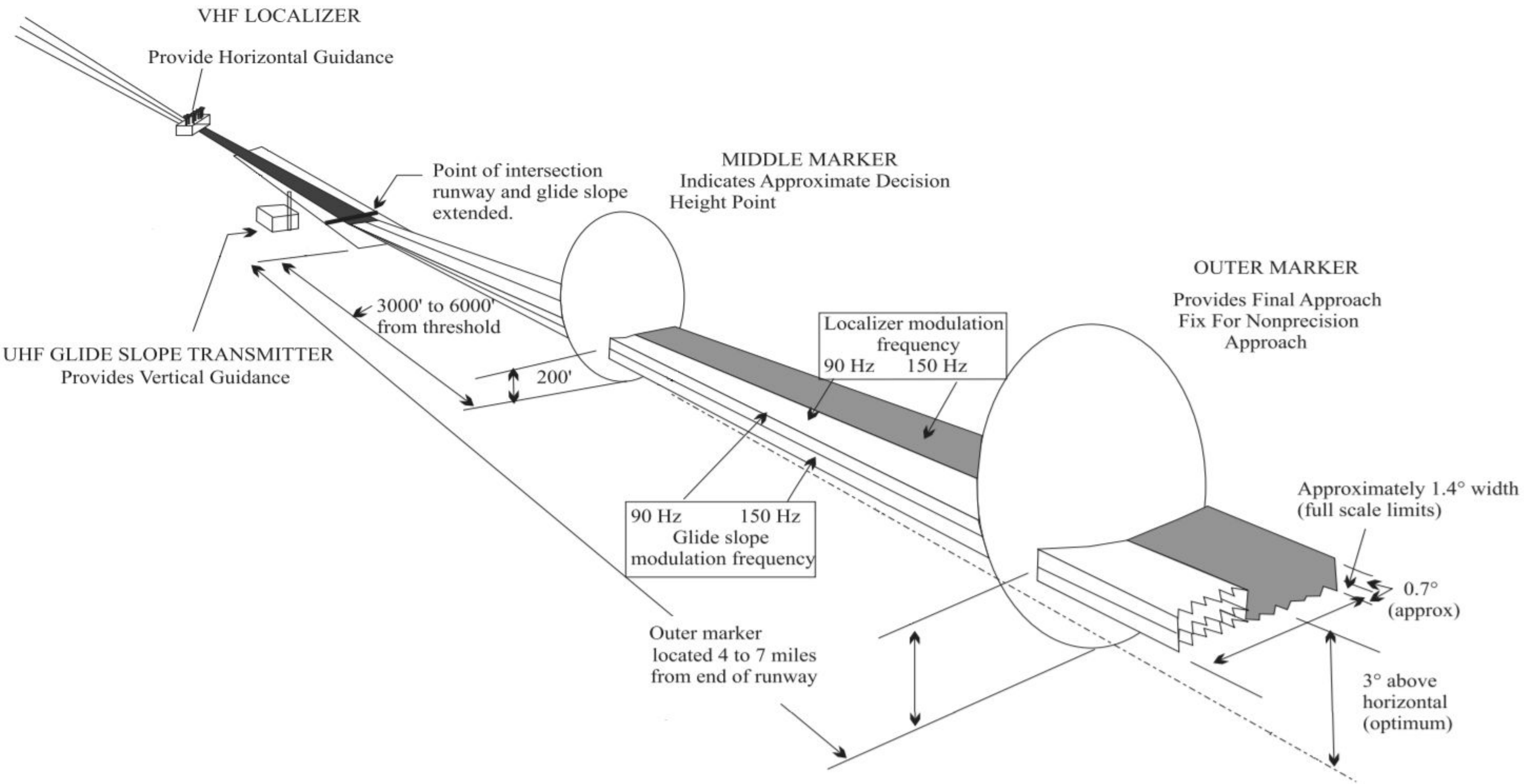
Today’s Navigation

- GNSS - predominantly GPS
- INS - Inertial Navigation System
- ILS - Instrument Landing Systems

INS Limitations

- Depending on age/model 0.5-1 nautical mile per hour
- Have to set the starting location
- Can reset using GPS during flight
  - If trust the GPS

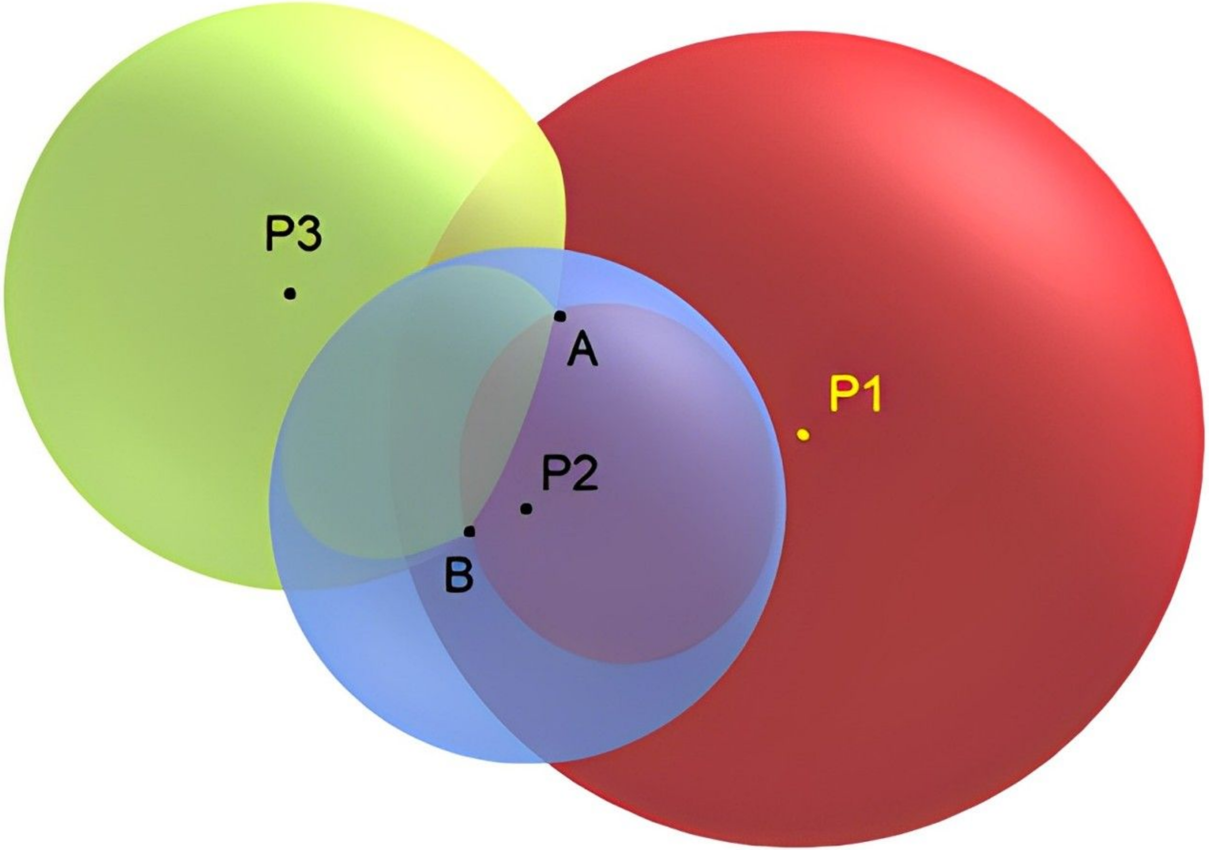
Instrument Landing System (ILS)


VHF LOCALIZER
Provide Horizontal Guidance
Point of intersection runway and glide slope extended.
MIDDLE MARKER
Indicates Approximate Decision Height Point
OUTER MARKER
Provides Final Approach Fix For Nonprecision Approach
Localizer modulation frequency
90 Hz 150 Hz
3000' to 6000' from threshold
UHF GLIDE SLOPE TRANSMITTER
Provides Vertical Guidance
200'
90 Hz 150 Hz
Glide slope modulation frequency
Approximately 1.4° width (full scale limits)
0.7° (approx)
Outer marker located 4 to 7 miles from end of runway
3° above horizontal (optimum)

From the Ground

- Primary Radar
- MLAT - Multilateration
    - TDoA - Time Difference of Arrival
    - Get the time of the first bit

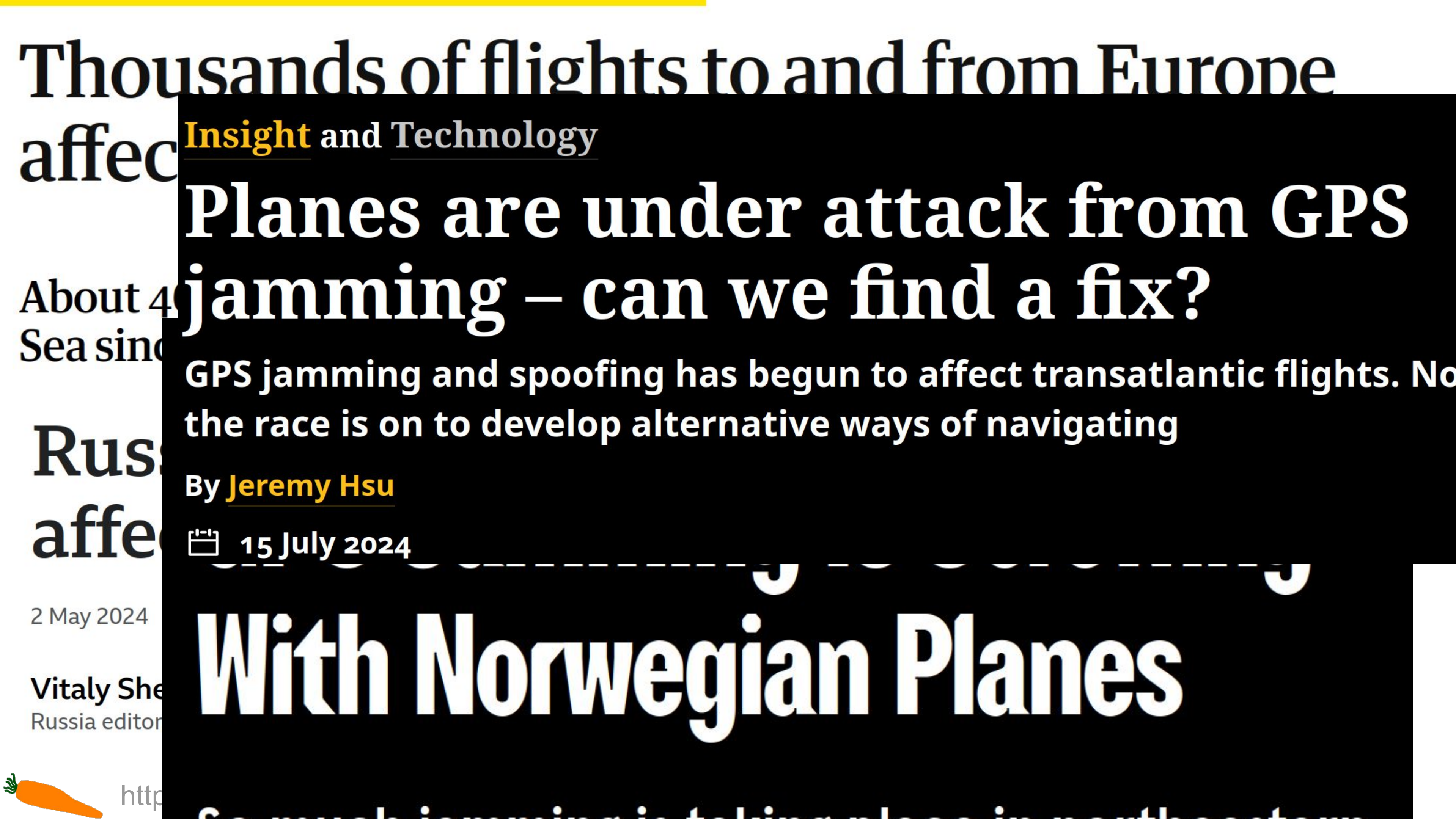
How MLAT works



Broadcasting Location

- ADS-B - Automatic Dependent Surveillance – Broadcast
  - Planes (& ground vehicles) broadcast their GPS or INS

What could go wrong?



Thousands of flights to and from Europe affec

About 4

Sea sinc

Russ

affe

2 May 2024

Vitaly She

Russia editor

Insight and Technology

Planes are under attack from GPS jamming – can we find a fix?

GPS jamming and spoofing has begun to affect transatlantic flights. No

the race is on to develop alternative ways of navigating

By Jeremy Hsu

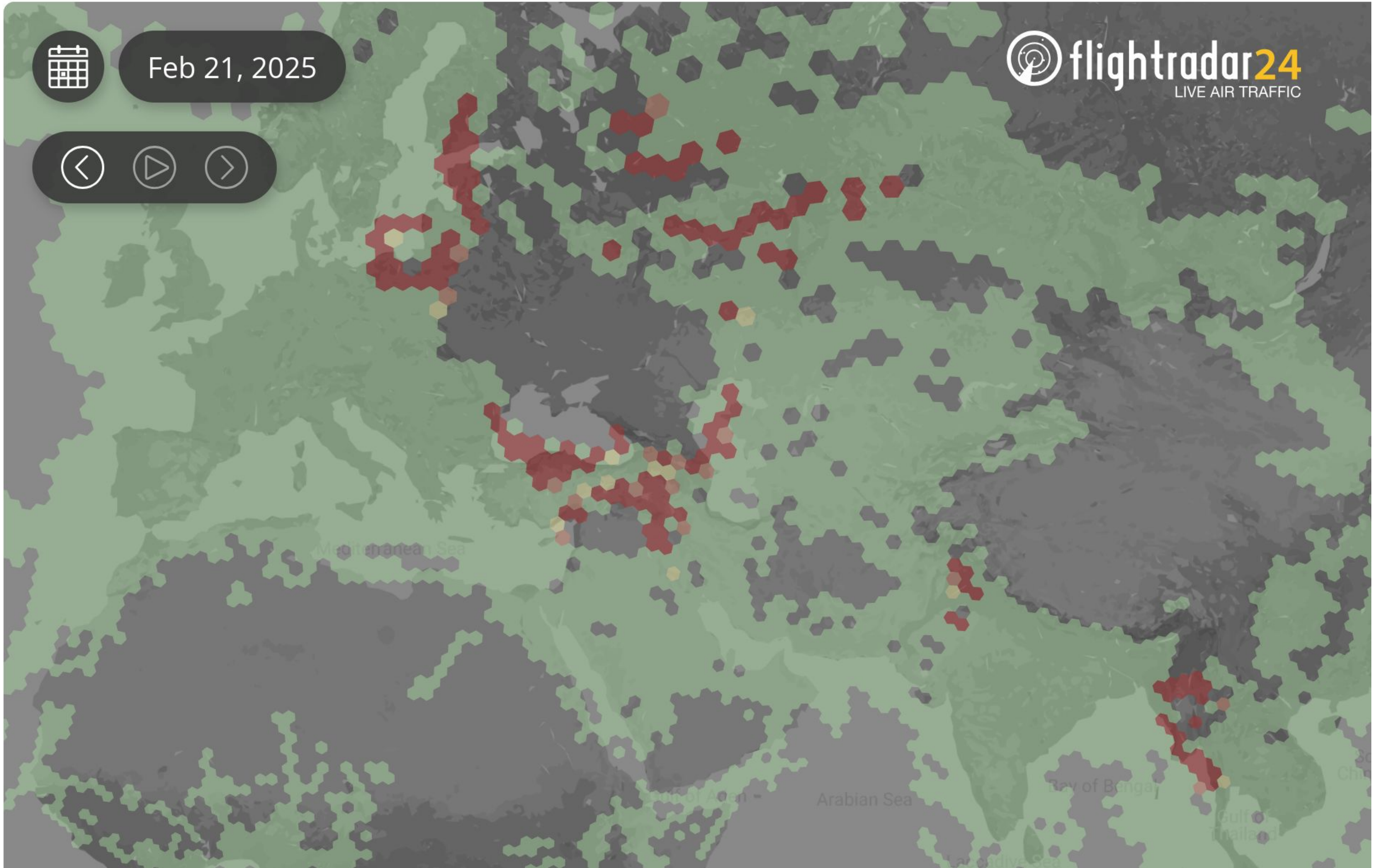
15 July 2024

With Norwegian Planes

So much jamming is taking place in northeastern

http

GPS jamming map



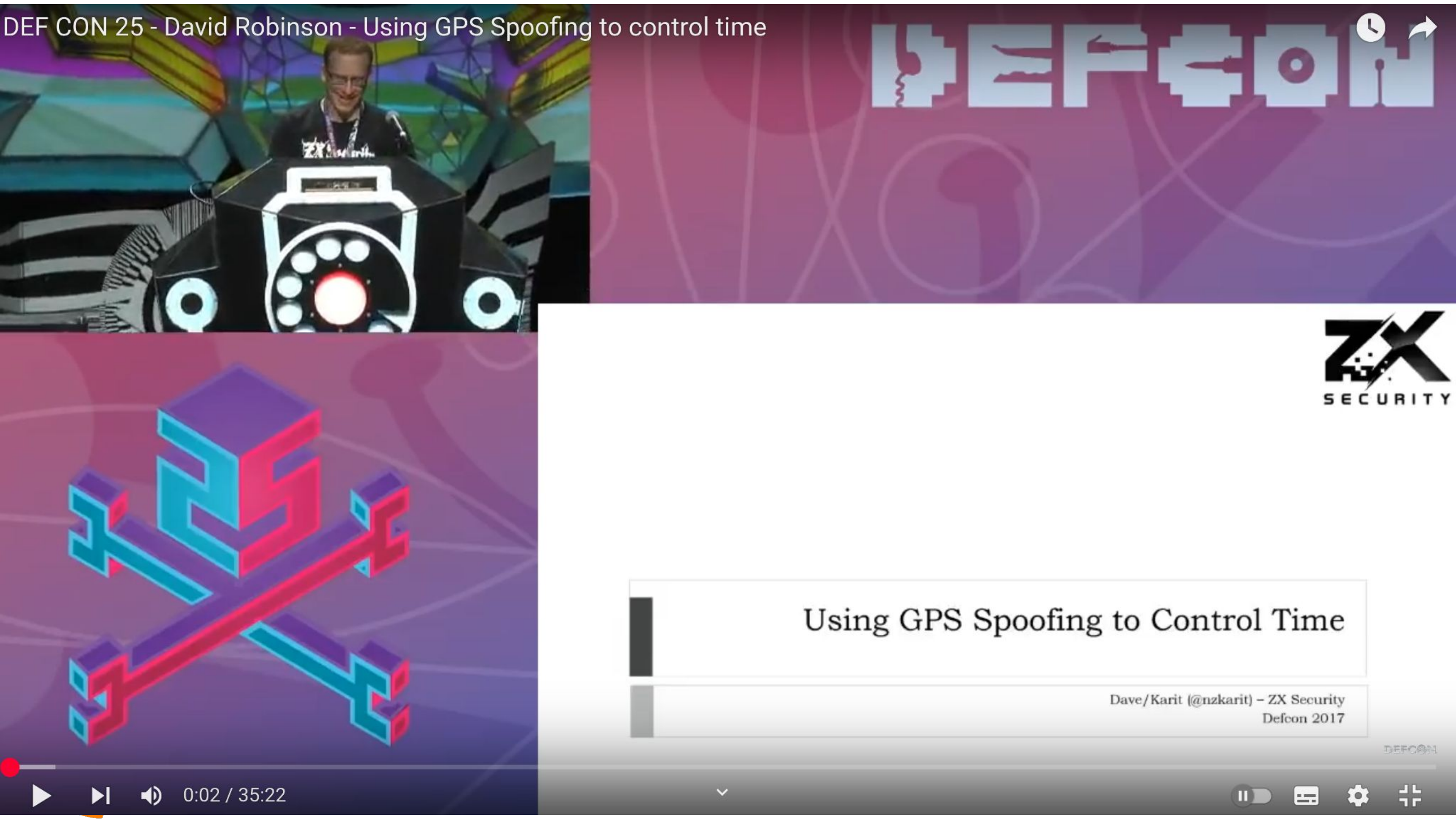
htt

How can planes tell?

- Sudden change in location
- Time jump

Spoofing vs Jamming

- Jamming is interference
  - GPS signal is in the noise floor
- Spoofing
  - Valid but wrong



DEF CON 25 - David Robinson - Using GPS Spoofing to control time

Using GPS Spoofing to Control Time

Dave/Karit (@nzkarit) – ZX Security
Defcon 2017

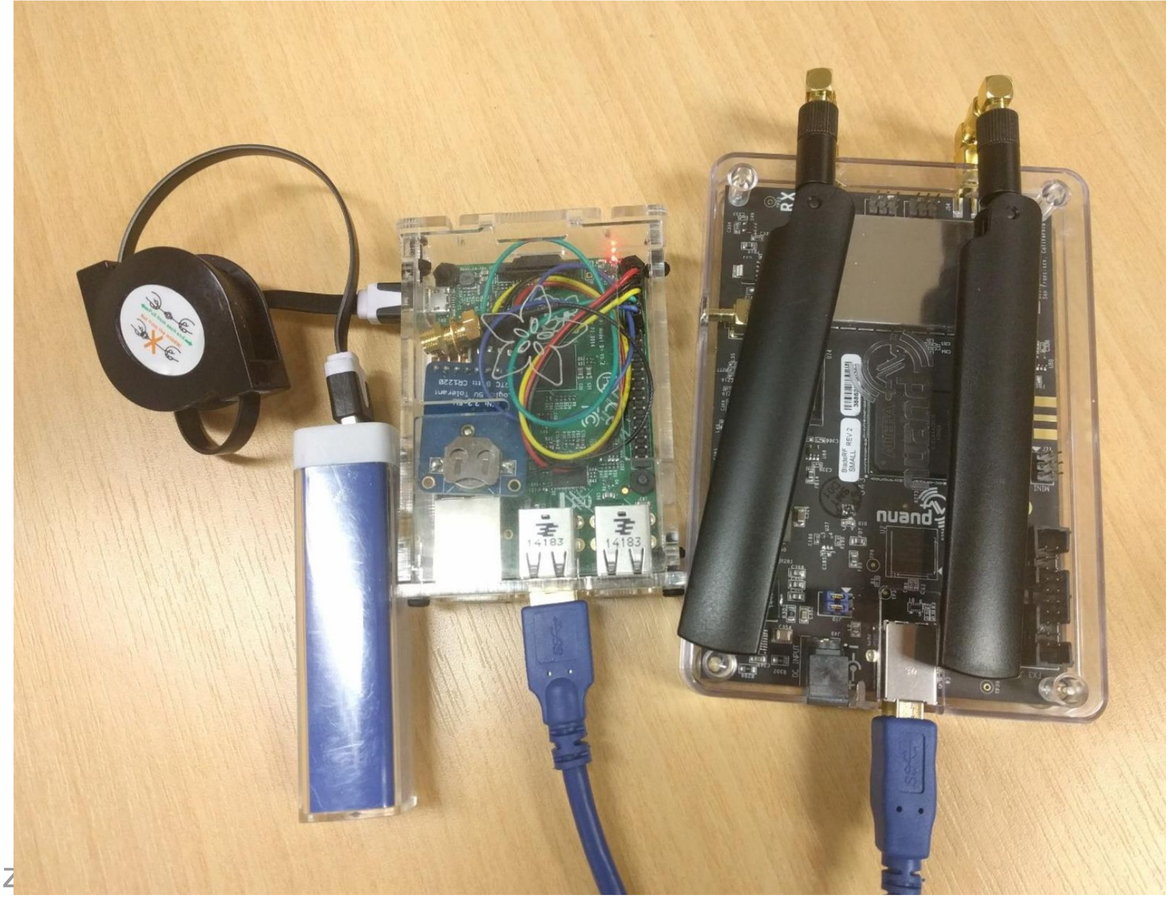
What this means?

- Planes don’t know where they are?
- Less optimal routes

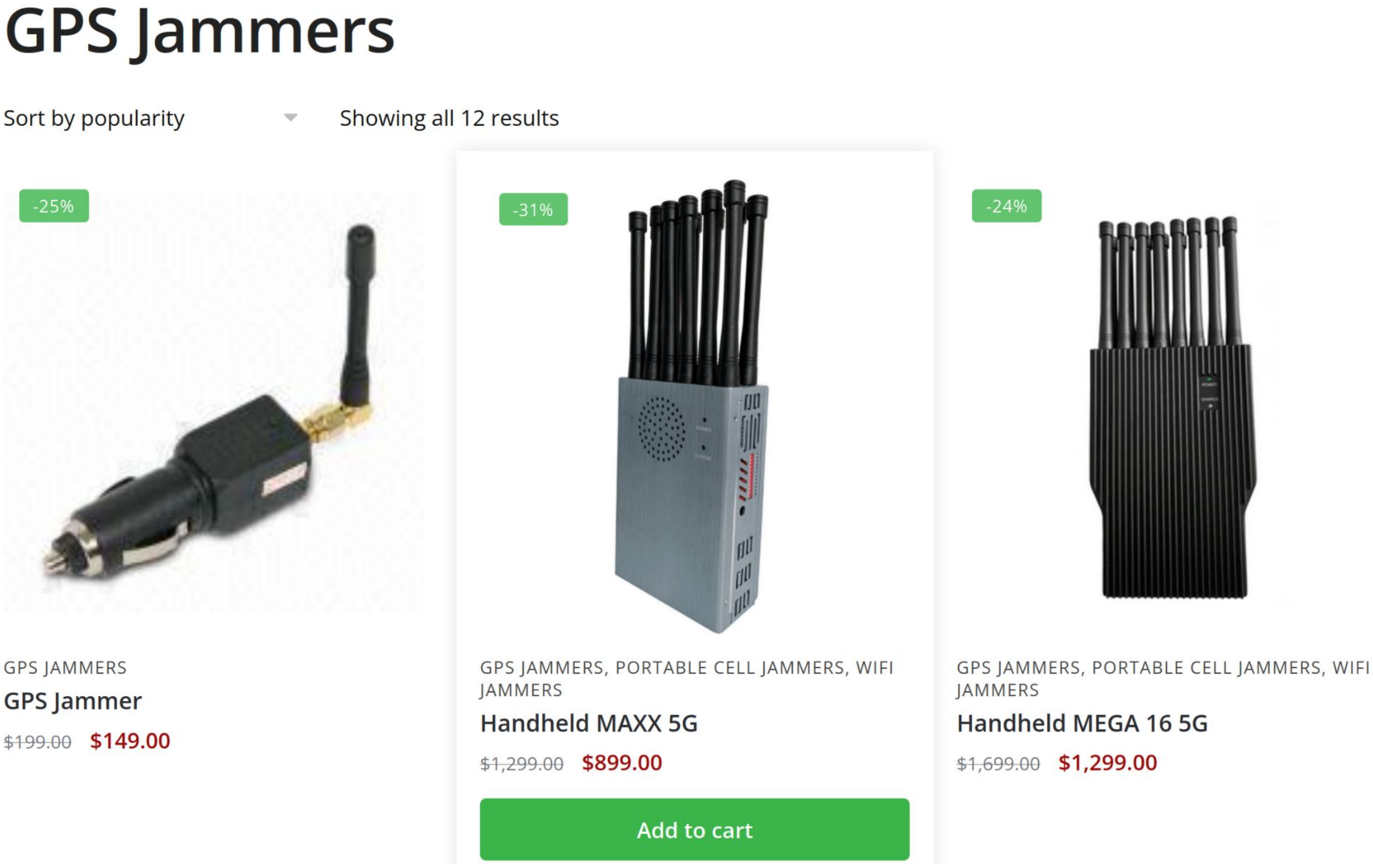
Off Course?

- Korean Airlines Flight 007
- 1 September 1983
- Off Course, got shot down
- Outcome GPS public service made available

How easy to spoof or jam?



Just buy a jammer



GPS Jammers

Sort by popularity

Showing all 12 results

-25%

GPS JAMMERS

GPS Jammer

~~$199.00~~ $149.00

-31%

GPS JAMMERS, PORTABLE CELL JAMMERS, WIFI JAMMERS

Handheld MAXX 5G

~~$1,299.00~~ $899.00

-24%

GPS JAMMERS, PORTABLE CELL JAMMERS, WIFI JAMMERS

Handheld MEGA 16 5G

~~$1,699.00~~ $1,299.00

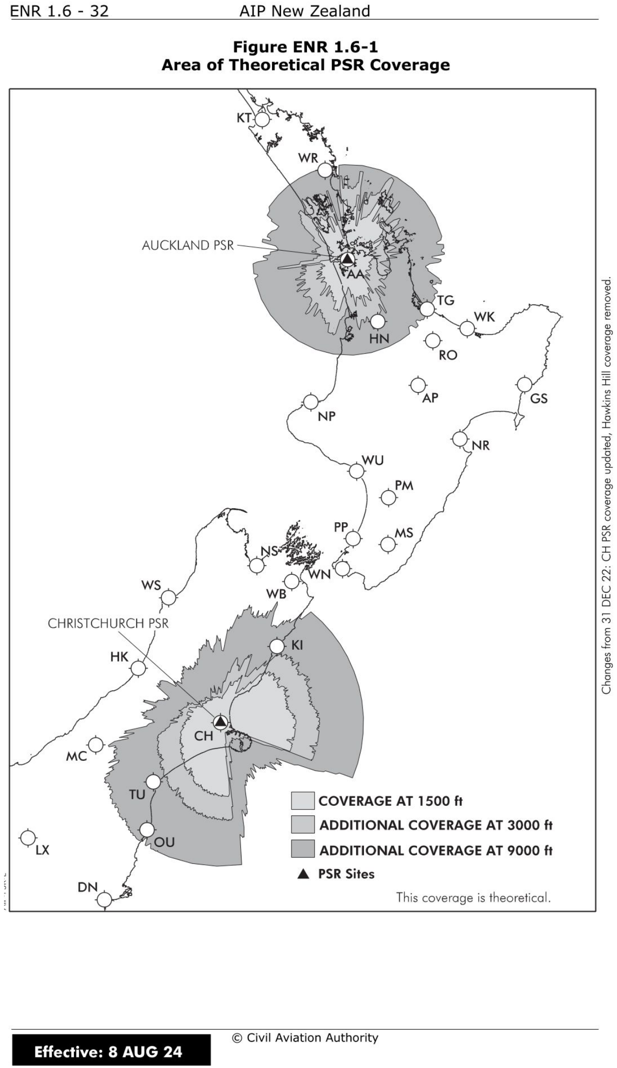
Saving Money

Costs

- VORs and Primary Radar is expensive
- To install
- To maintain

- Decommission, Not Fix, Build New Stuff

NZ Radar Coverage



ENR 1.6 - 32 AIP New Zealand

Figure ENR 1.6-1
Area of Theoretical PSR Coverage

Changes from 31 DEC 22: CH PSR coverage updated, Hawkins Hill coverage removed.

Effective: 8 AUG 24

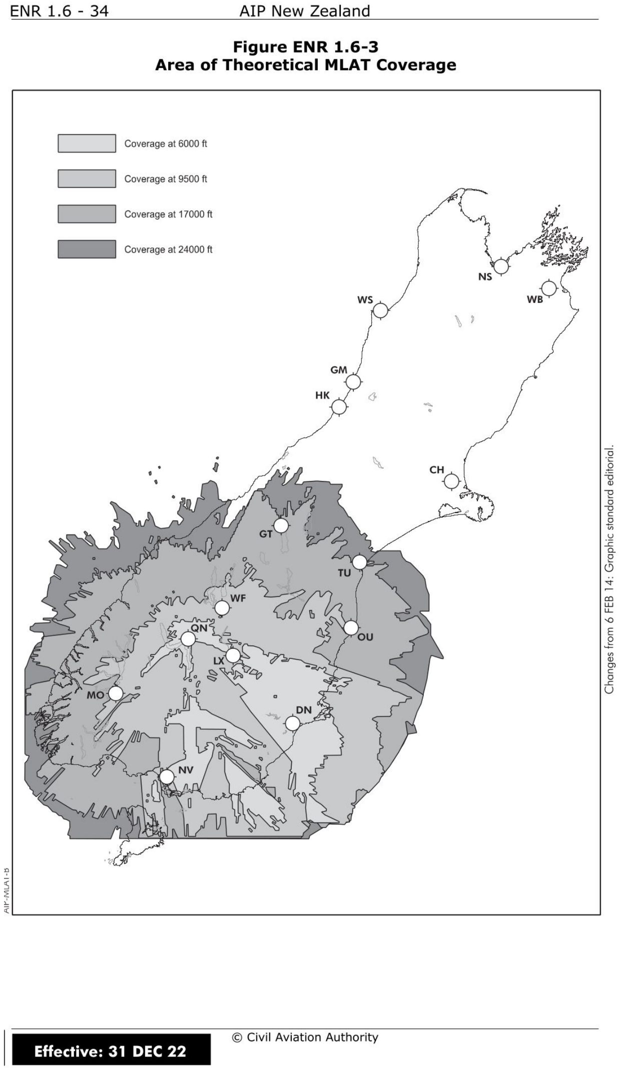
So what are they doing?

- ADS-B
  - Where plane to tells ATC where it is
  - Plane has to have ADS-B Out
  - But if the plane doesn’t know where it is?

MLAT

- Coverage still isn’t there
- Still needs plane to be at least Mode-S

NZ MLAT Coverage



ENR 1.6 - 34 AIP New Zealand

Figure ENR 1.6-3
Area of Theoretical MLAT Coverage

AIP-MLAT-B

Changes from 6 FEB 14: Graphic standard editorial.

Effective: 31 DEC 22

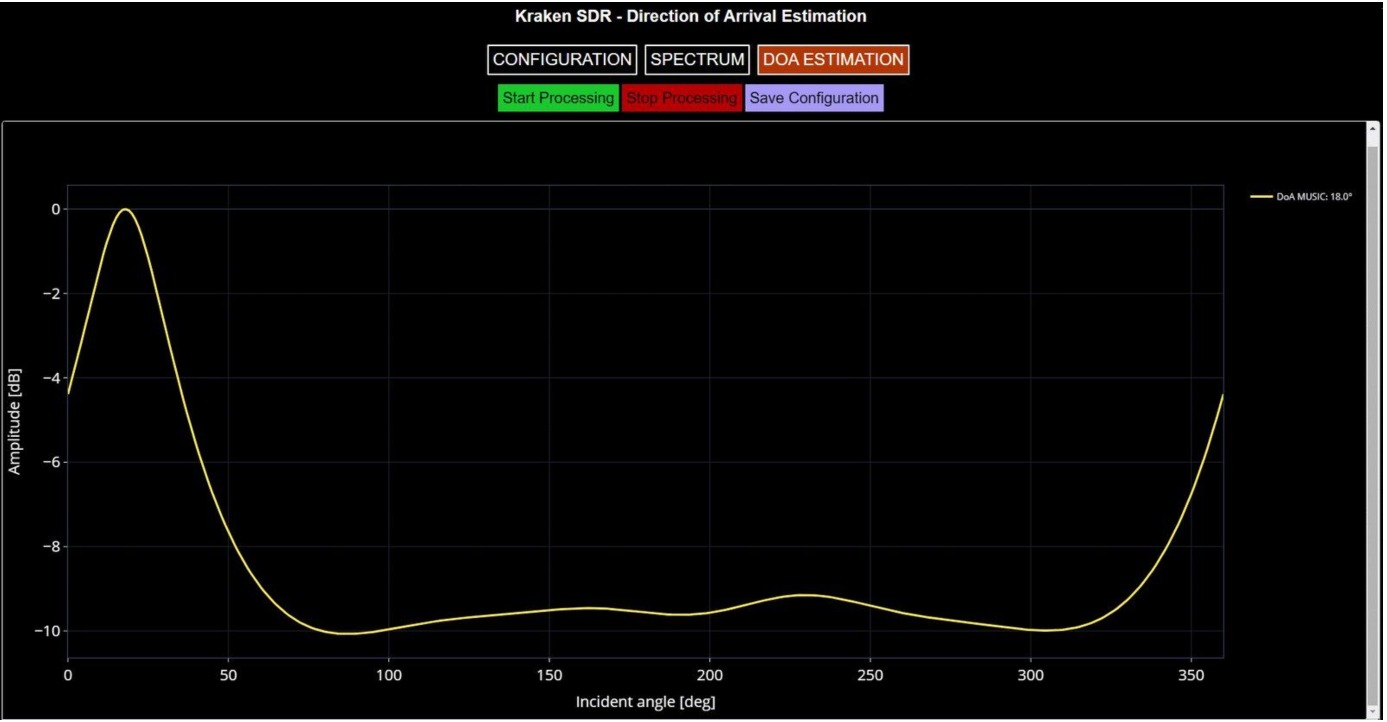
© Civil Aviation Authority

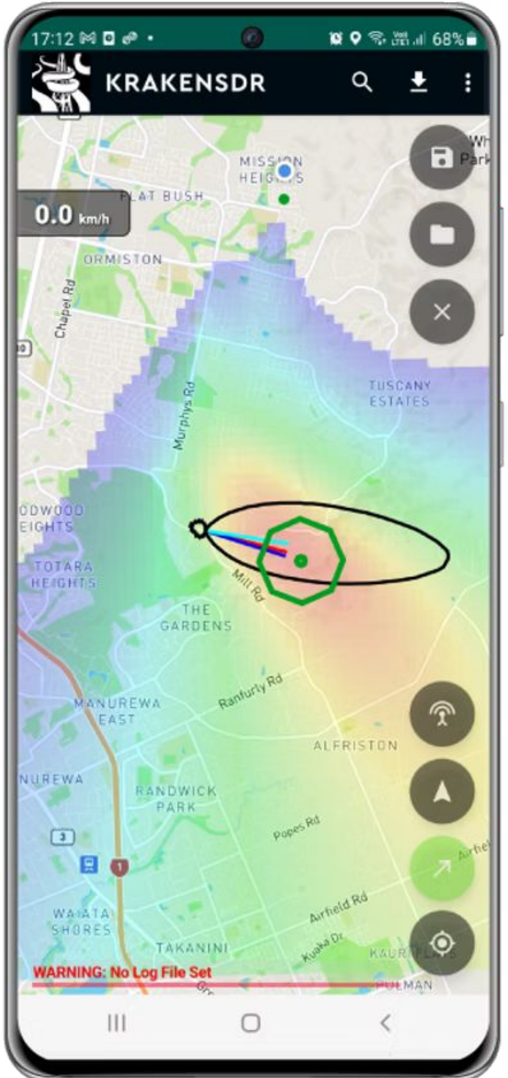
https://karit.nz

Where to Next? - Direction Finding

Direction Finding

Direction Finding





https://karit.nz

How this DF works

- Space the 5 antennas out based on frequency tracking in a circle
- From the different timing/phase of signal each antenna sees can calculate direction

- Older forms sweeped a directional antenna

Similar to MLAT

- Can use it similar to MLAT
- Benefit can use analog not just digital
    - Audio, ACARS and ADS-B/Mode-S

Costs

- Less than a US$1000
- But aviation so add a zero or two
- Plus the backend systems

Pros for Planes

- Can get fixes off any fixed radio
  - TV, Radio
  - Similar to ADF/VOR but someone else is paying
  - Cross reference location
- Could track were other planes are

Pros for Planes

- TV and FM ground based and high powered
  - Not going to jam or overpower like GNSS
  - If jammed everyone has the tracking kit

Cons for Planes

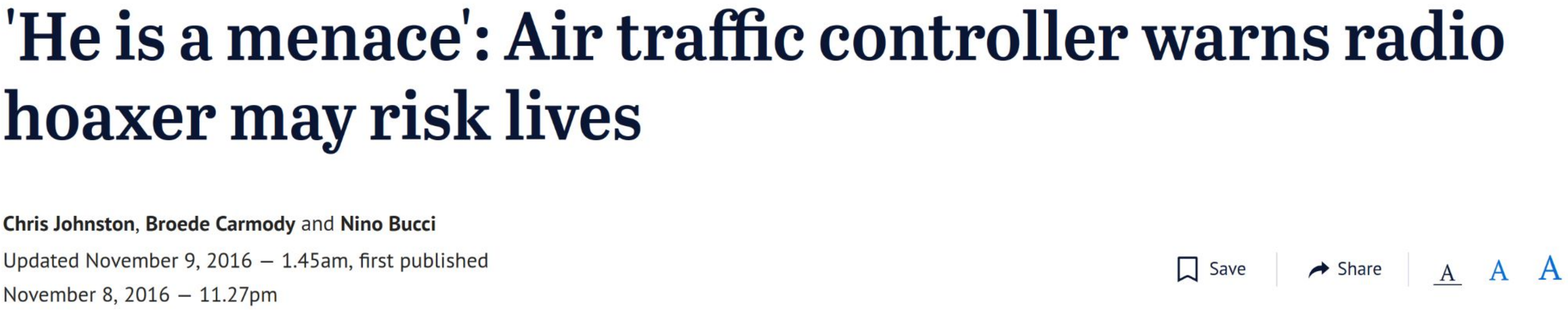
- Need a set of radios per frequency monitor
- Hard to get optimal layout for a range of frequencies
- Only over land and coastal

Pros fro ATC

- Can direction find off ADS-B/Mode-S on 1090MHz
- Additionally could direction find audio
  - Though not continuous
- Can triangulate if have multiple sites
  - Don’t need the low latency for timing

Pros for ATC

- Locate fake people on frequency



'He is a menace': Air traffic controller warns radio hoaxer may risk lives

Chris Johnston, Broede Carmody and Nino Bucci

Updated November 9, 2016 — 1.45am, first published November 8, 2016 — 11.27pm

Cons for ATC

- Works best in horizontal plane
  - At a distance angle of different altitudes not as great
  - Would need second array in a vertical plane
- More equipment at each site compared with MLAT

Cons for ATC

- If using voice radio no ID

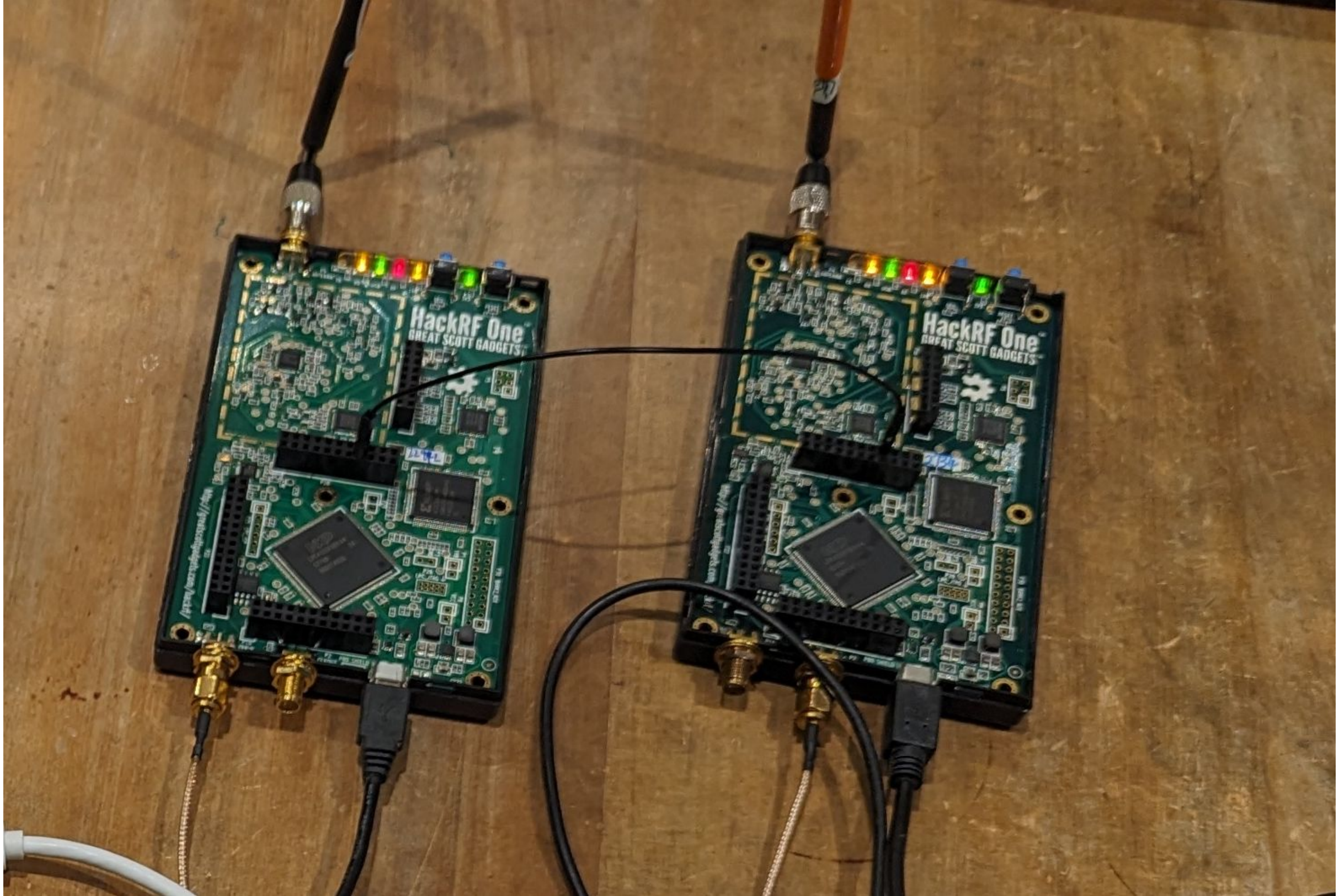
Where to Next? - Passive Radar

Passive Radar

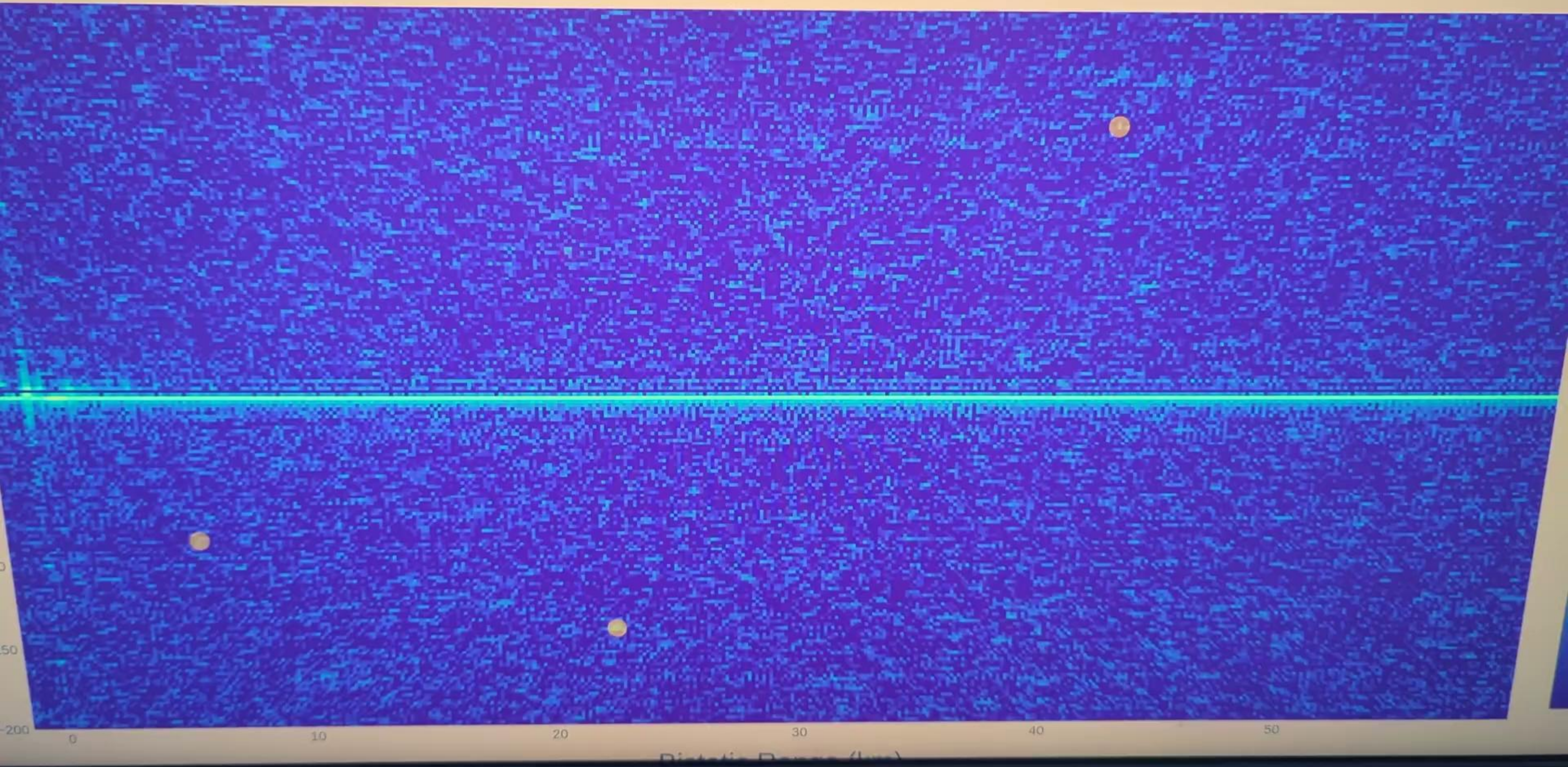
- Uses existing FM, TV, Cell Base Stations
- Something with a constant carrier
- Need a fix location for receiver
  - So only helpful for ATC

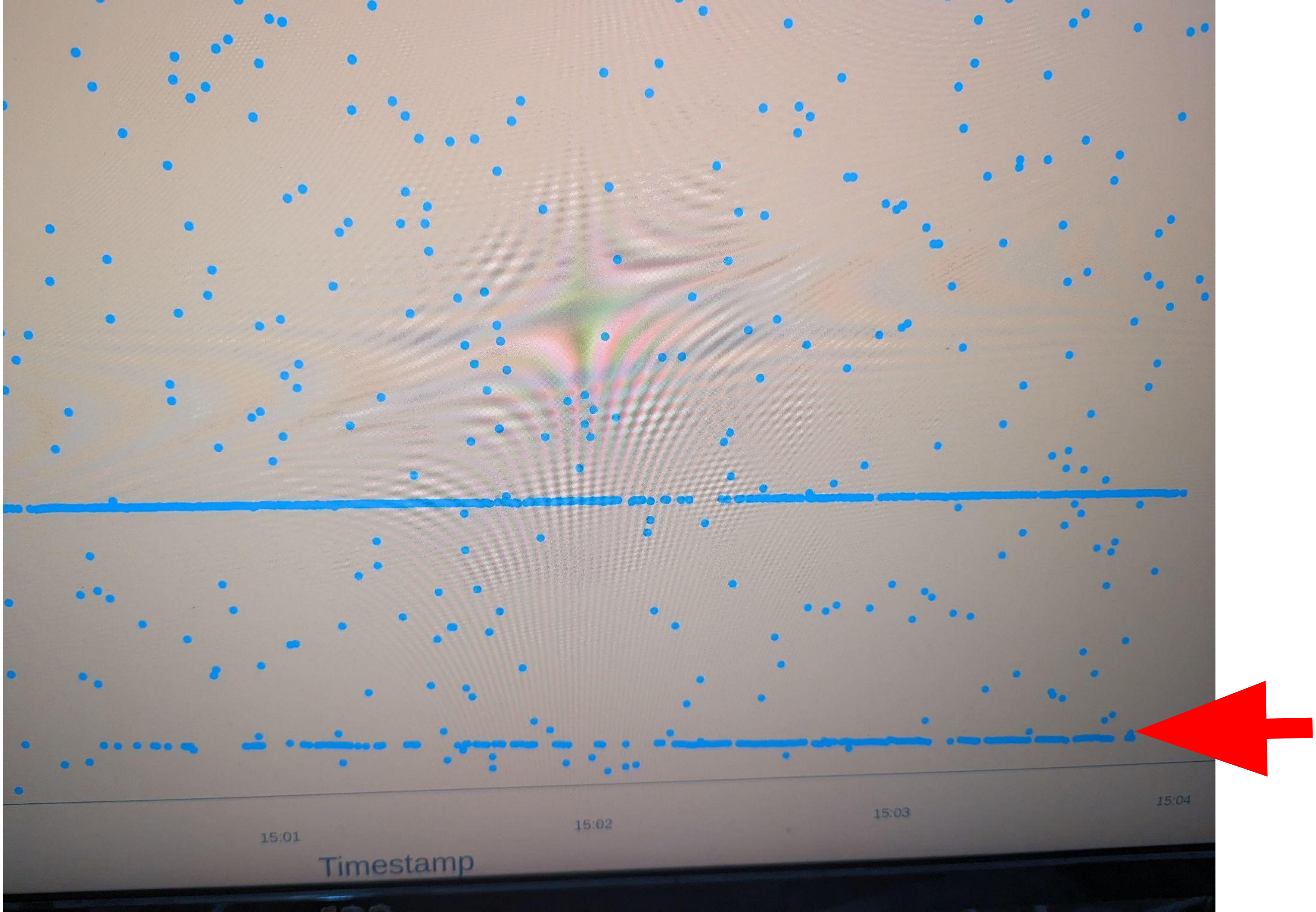
Cool Physics

- Benchmark the spectrum
- While planes move through the radio waves
  - Reflect
  - Change wavelength
  - Change polarisation
- Can get location, speed and direction


HackRF One
GREAT SCOTT GADGETS
HackRF One
GREAT SCOTT GADGETS

RADAR CONTROLLER





https

Pros for ATC

- From one location can get a fix
- Needs less radios than DF (2 vs 5)
- TV, FM or Cell orgs provide the expensive broadcast portion
- Can tie multiple sites or multiple frequencies together

Cons for ATC

- ITAR Restrictions
    - International Traffic in Arms Regulations
    - KrackenSDR had Passive Radar & was pulled
    - Other examples exist

Where to Next? - eLORAN

eLORAN

- Enhanced Long Range Navigation
- LORAN
    - Old Decommissioned Tech
- With GPS jamming investigation

How eLORAN works

- All towers in sync
- Different in time/phase can infer location
- <10m accuracy

- 2017/2018 Black Sea and North Korean interference

Pros Planes

- Strong signal hard to drown out
- <10m good for navigation not landing

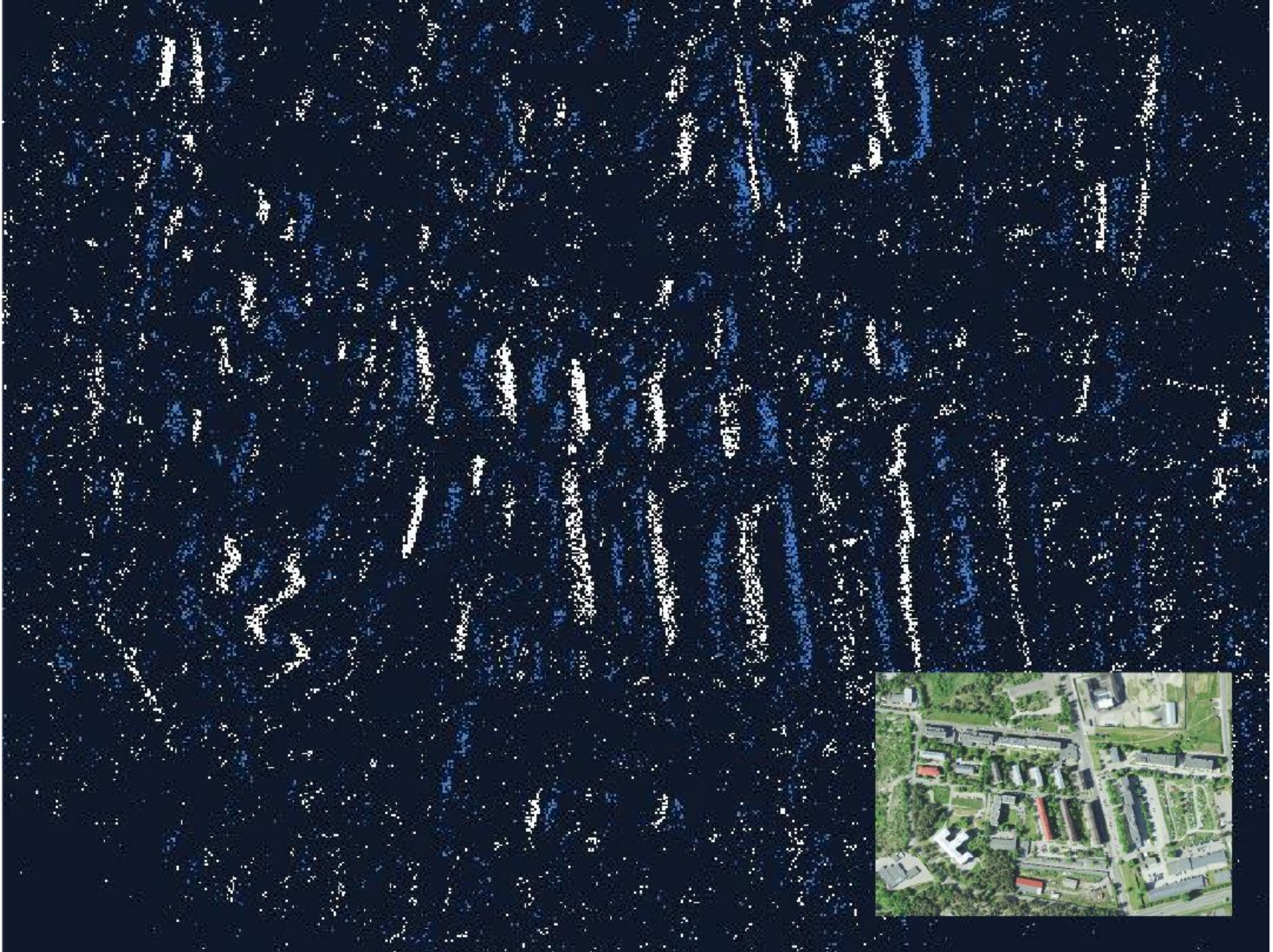
Cons Plane

- Not implemented only talk
- 1200km from coast

Where to Next? - Earth Fingerprinting

Earth Fingerprinting

- Build a fingerprint of earth terrain
- Use a camera to match



https

Pros for Planes

- Hard to change terrain at scale

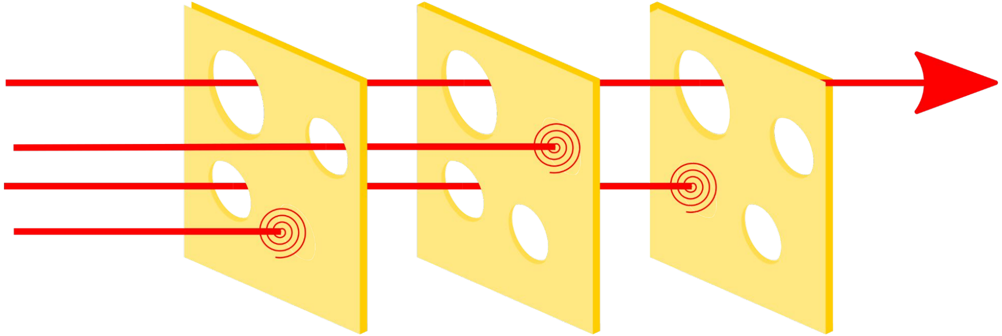
Cons for Planes

- Need to see the ground
- Need to be over land

Wrapping up

Conclusion

- No easy options
- But multiple redundant method
- Land and Coastal easier
  - But less jamming over the ocean

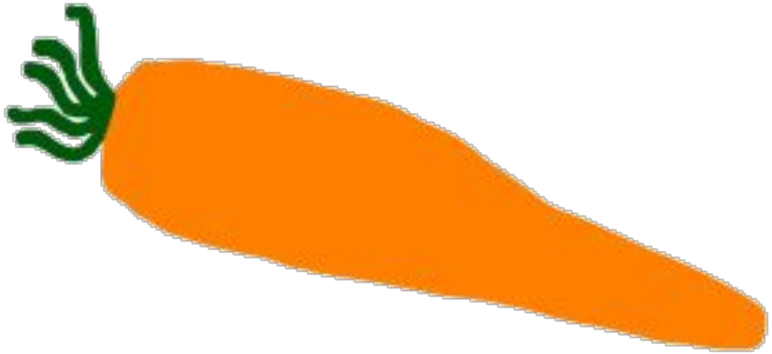


Where to next?

- Aviation Regulators
- Airliner Manufacturers/Part supplies

Hopefully I have covered

- How Aviation Navigates
- Attacks on the Aviation Navigation
    - Pilots’ Perspective
    - Air Traffic Control’s Perspective
- What can we do about it?



Thanks

Contact:
https://karit.nz/social

Photo Credits

https://upload.wikimedia.org/wikipedia/commons/6/61/ILS_diagramsimplified.png
https://en.wikipedia.org/wiki/Trilateration#/media/File:3D_Trilateration.jpg
https://www.theguardian.com/business/2024/apr/22/thousands-of-flights-to-and-from-europe-affected-by-suspected-russian-jamming
https://www.bbc.com/news/articles/cne900k4wvjo
https://www.wired.com/story/gps-jamming-is-screwing-with-norwegian-planes/
https://www.newscientist.com/article/2439560-planes-are-under-attack-from-gps-jamming-can-we-find-a-fix/
https://www.flightradar24.com/data/gps-jamming
https://www.youtube.com/watch?v=isiuTNh5P34
https://www.thesignaljammer.com/product-category/gps-jammers/
https://www.aip.net.nz/
https://www.aip.net.nz/
https://www.crowdsupply.com/krakenrf/krakensdr
https://www.crowdsupply.com/krakenrf/krakensdr
https://www.krakenrf.com/
https://www.auvsi.org/decoding-earths-fingerprint-advanced-navigation-and-nileq-collaborate-breakthrough-resilient
https://en.wikipedia.org/wiki/Swiss_cheese_model#/media/File:Swiss_cheese_model_textless.svg