

GNSS Protection Overview 2017

Michael Jones MEng(Hons) CEng MIET FRIN
Senior Consultant Engineer & Capability Lead
michael.jones@roke.co.uk



About Roke

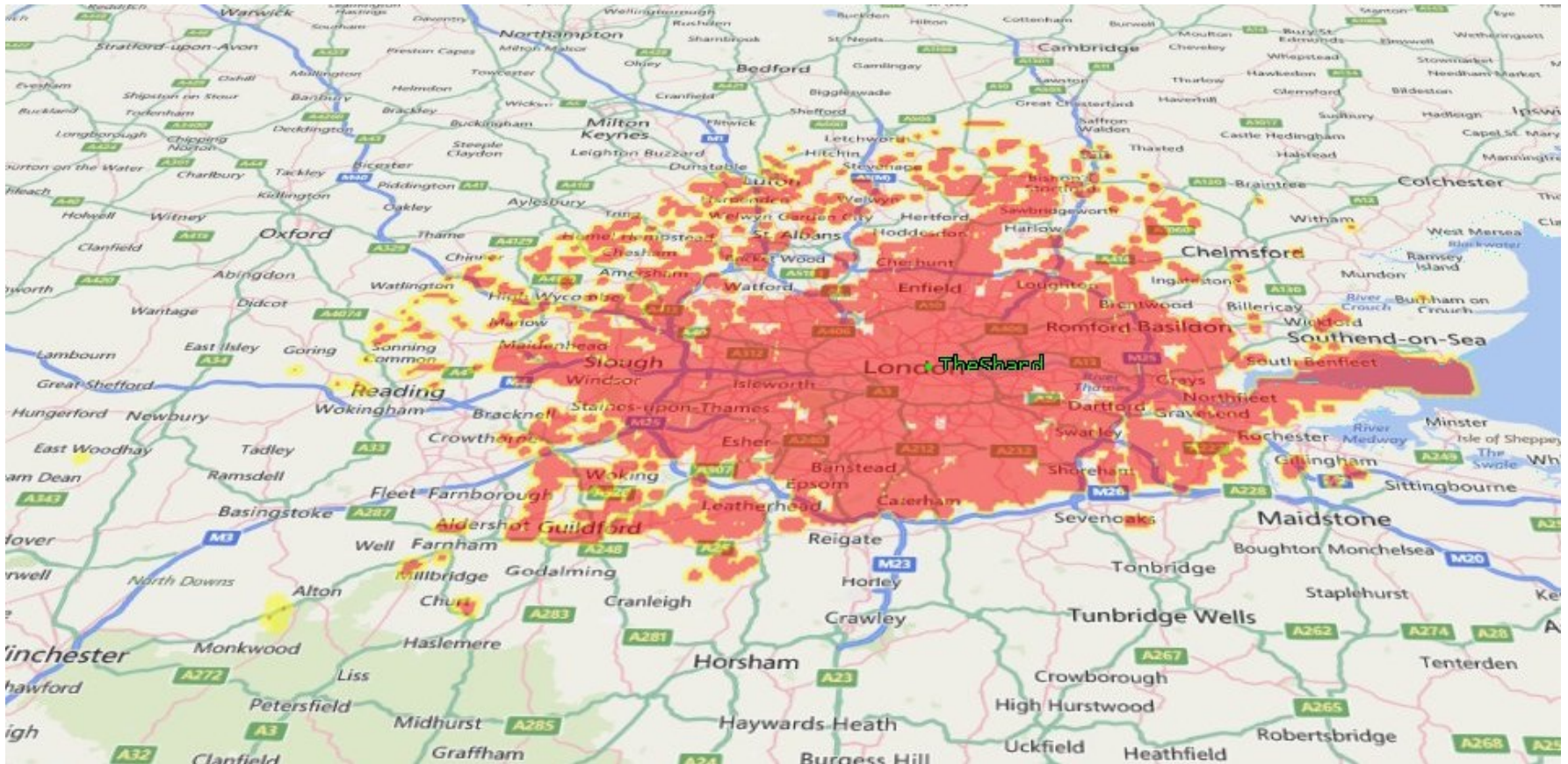
- 22 acre facility in the UK.
- Defense, National Security, and Commercial business units.
- Over 350 security-cleared engineers.
- World centre of excellence in electronic warfare, including navigation warfare.



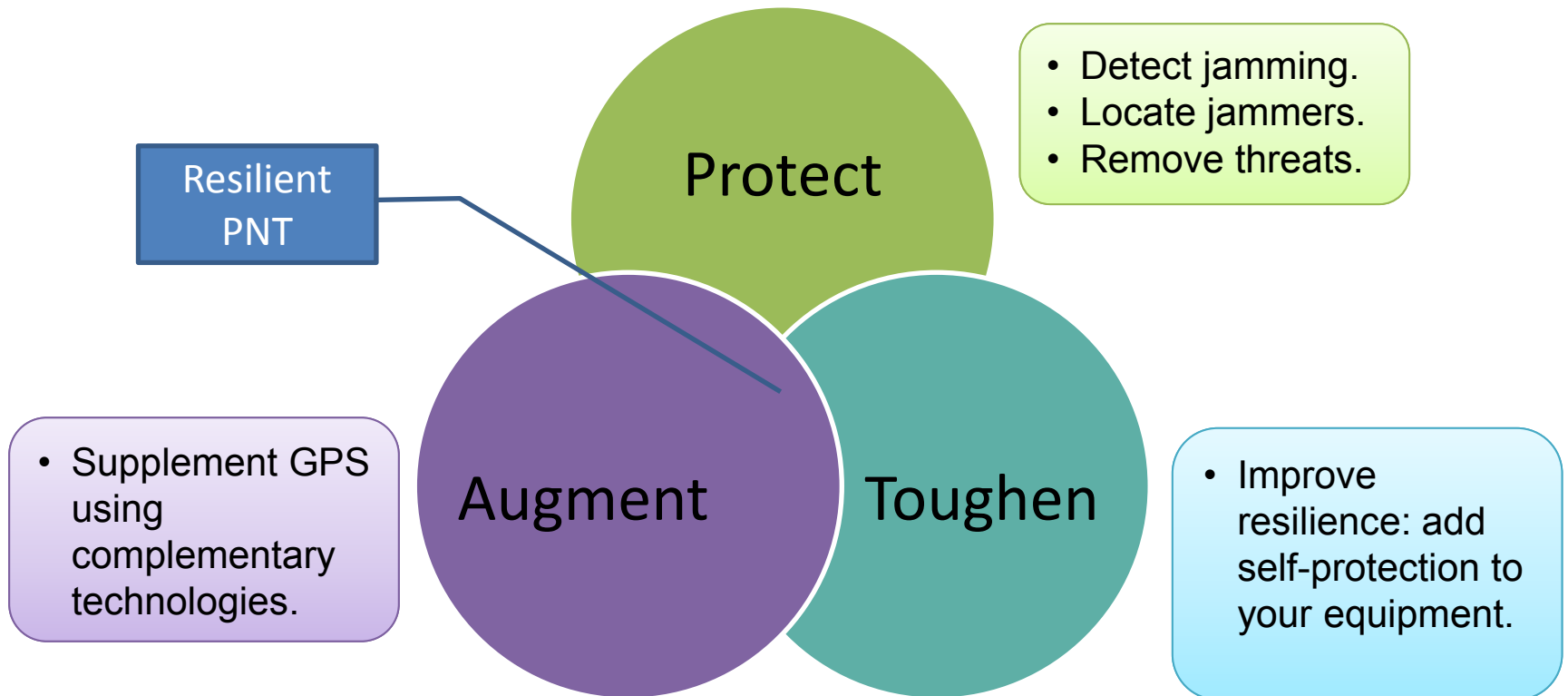
Licensed to perform open-air jamming and spoofing exercises

The Civilian Battlefield

- What could happen? Let's take a 100W jammer up the Shard building in London.

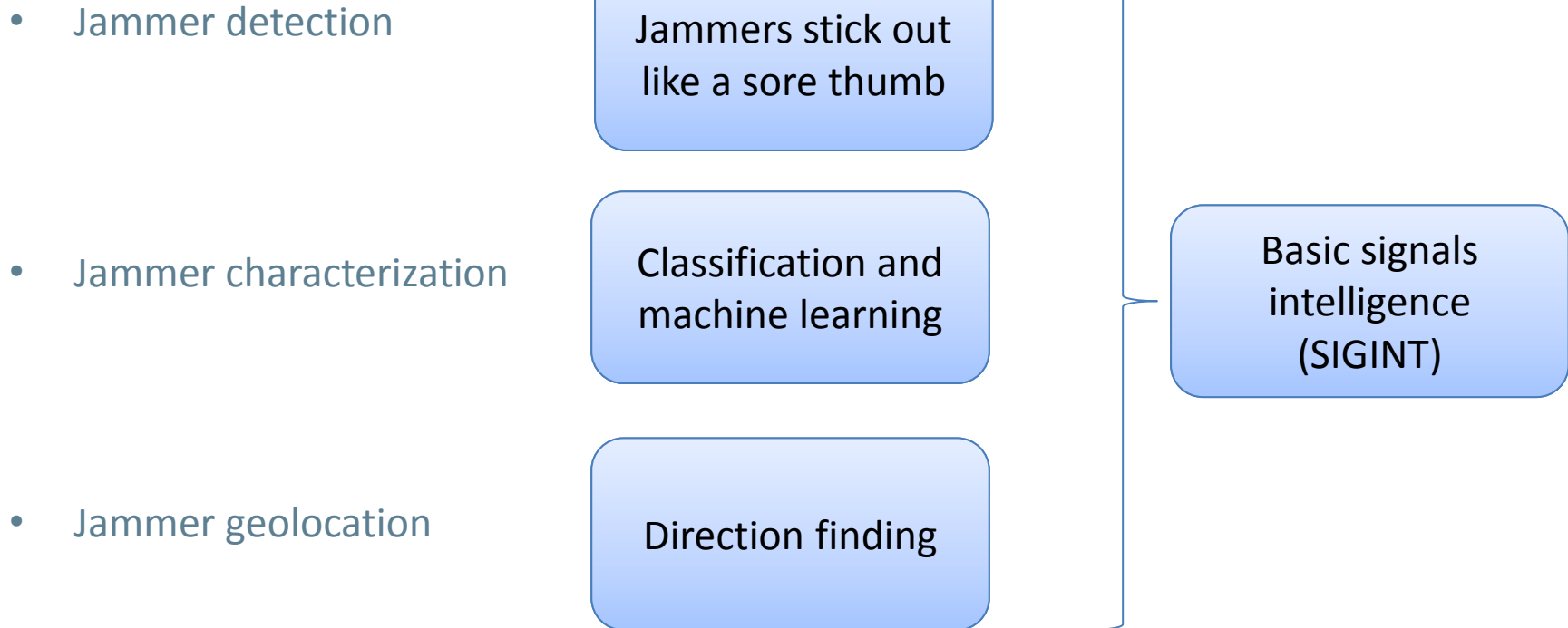


GPS Protection Overview



- This presentation will cover examples of the latest “protect” and “toughen” technology.

Jammer Detection and Geolocation



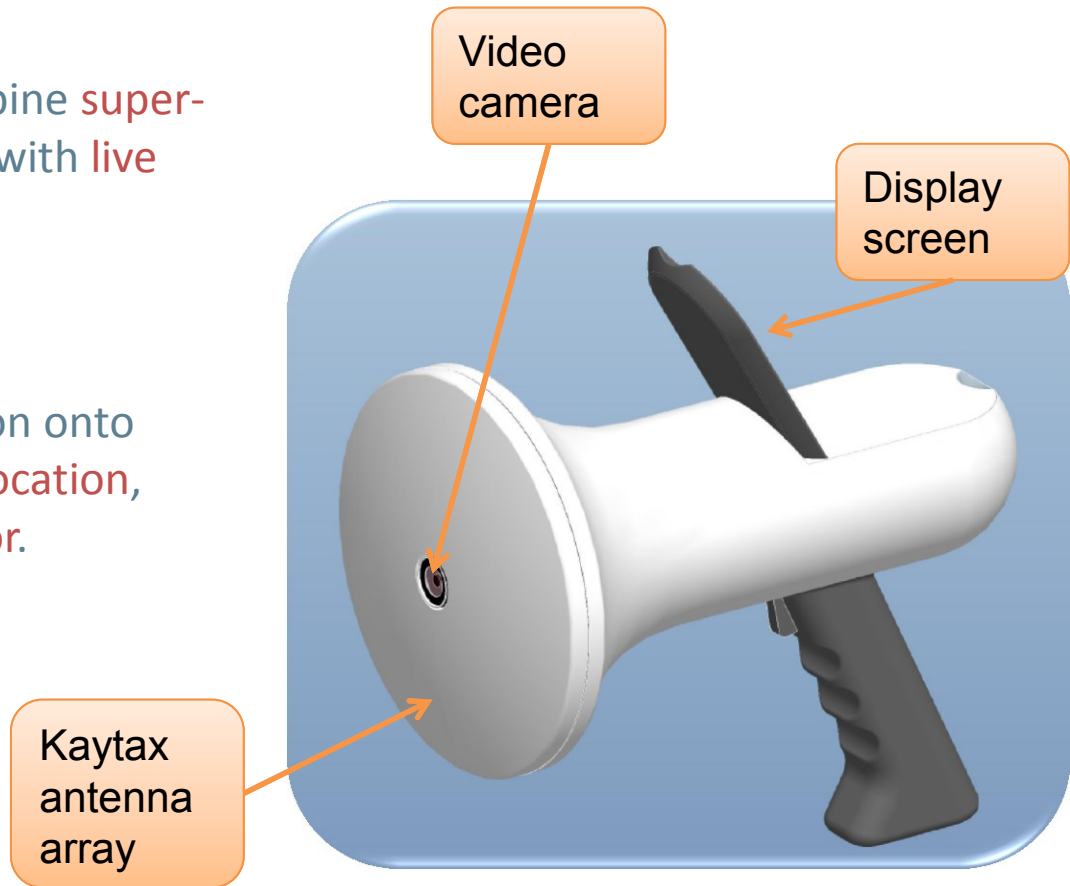
This is all classic EW, and well-understood technology.

Augmented Reality Jammer Geolocation

- The current trend is to combine **super-resolution direction finding** with **live video**.
- Projecting the signal direction onto video gives **pseudo-3D geolocation**, from a **single portable sensor**.



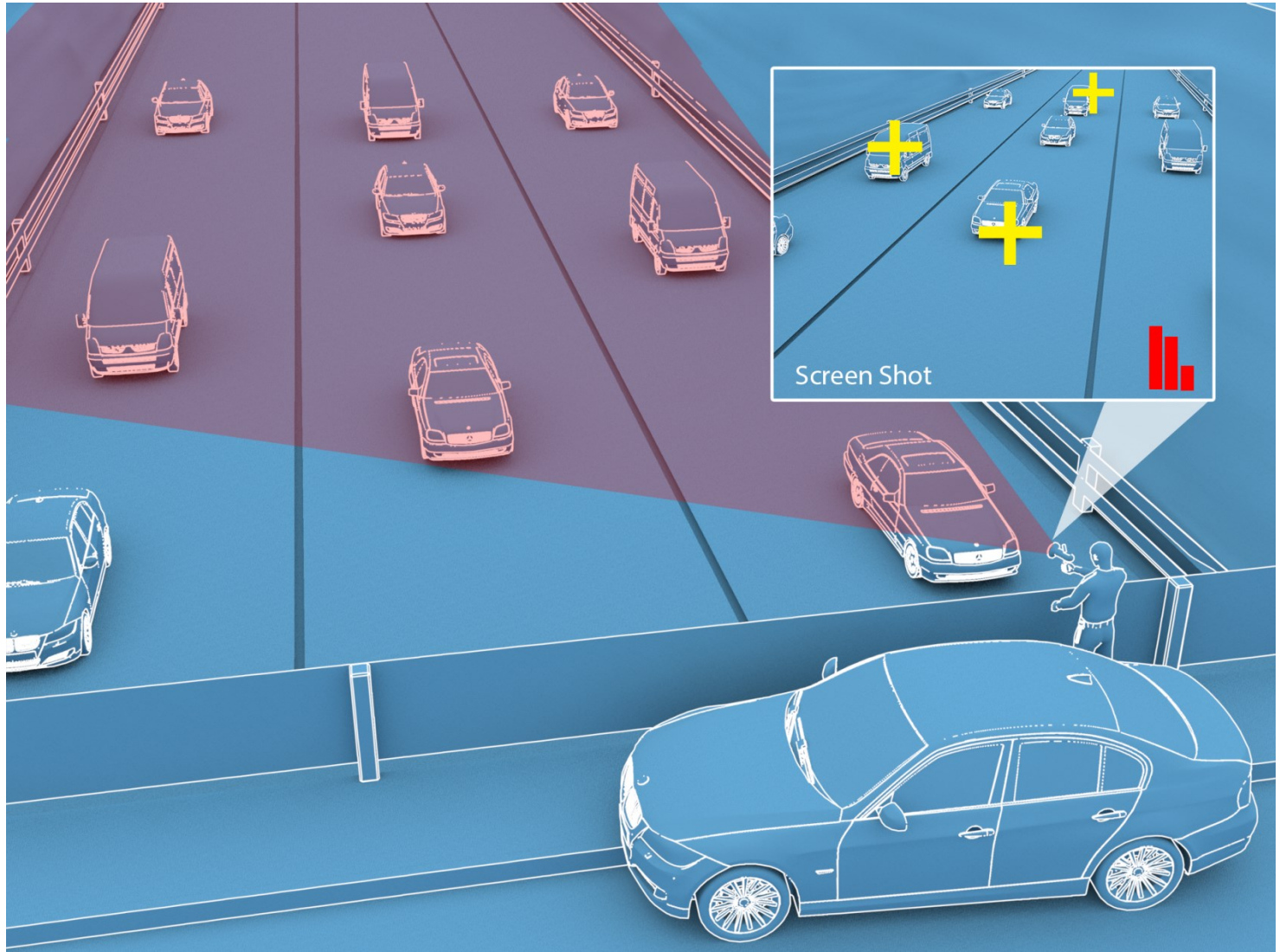
Current technology demonstrator



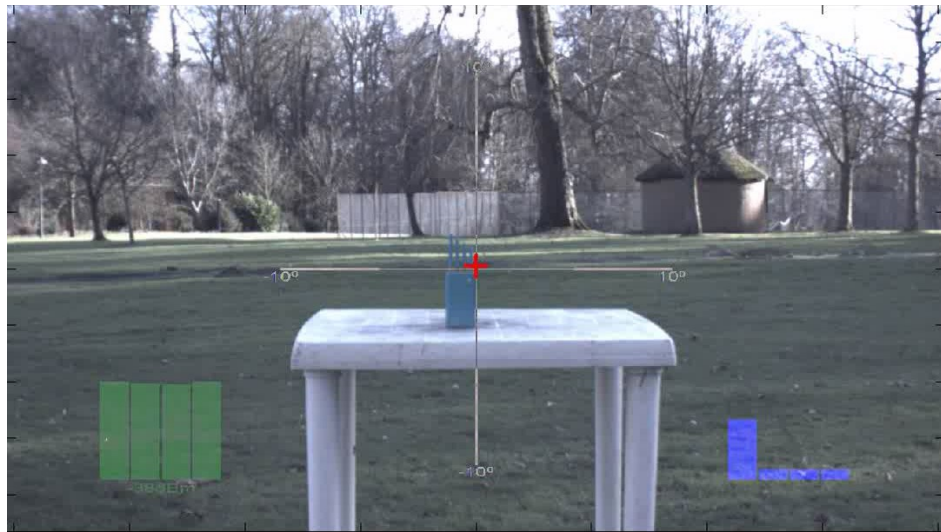
Product Concept

Augmented Reality Jammer Geolocation

- Crosshairs overlaid on jammers.
- Real-time operation.
- Multiple simultaneous jammers.



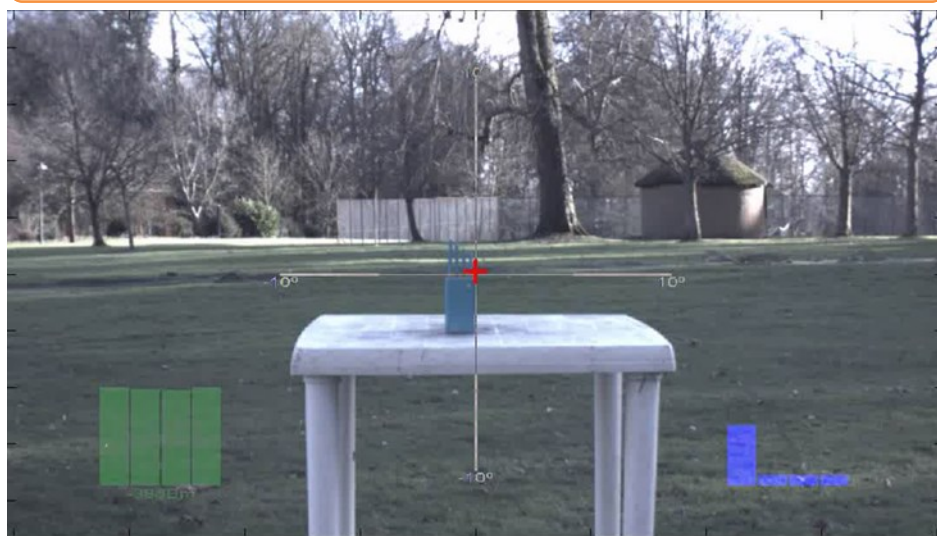
Augmented Reality Geolocation in Action



Augmented Reality Geolocation in Action

- It works extremely well...

Jammer on a table



Car with jammer



- The technology could be adapted to geolocate spoofers

Anti-Jam: the obvious, cheap and easy

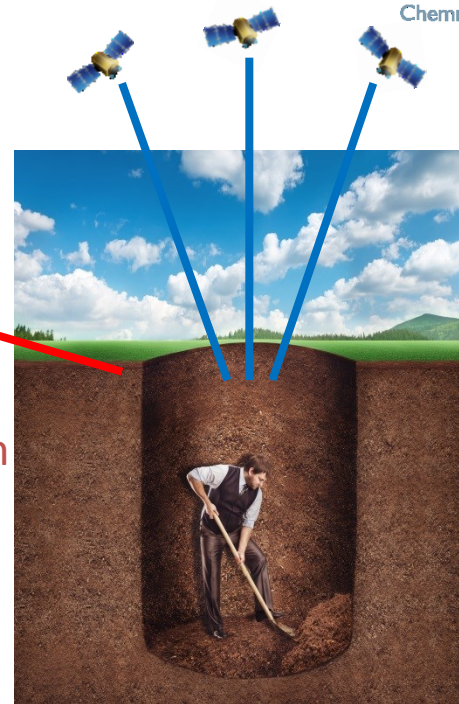


Choke ring or ring nuller

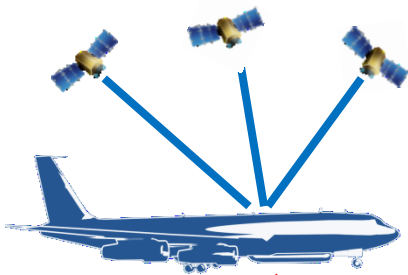
Dig yourself a hole...



~20 dB protection



Give yourself
some height...



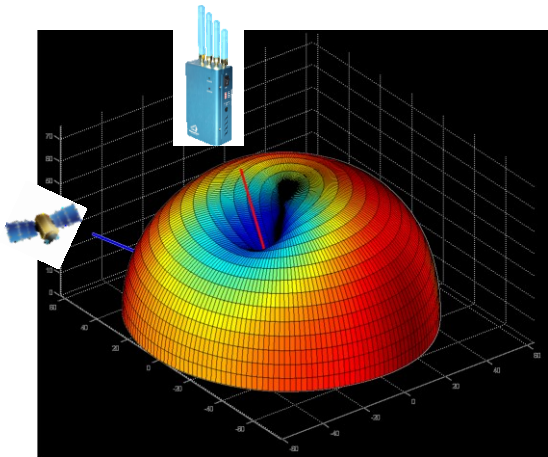
~100 dB protection



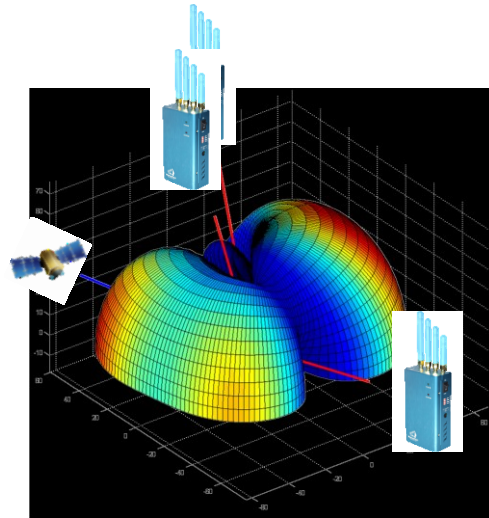
Simple steps can give you
significant protection from
jamming.

Anti-Jam Technology

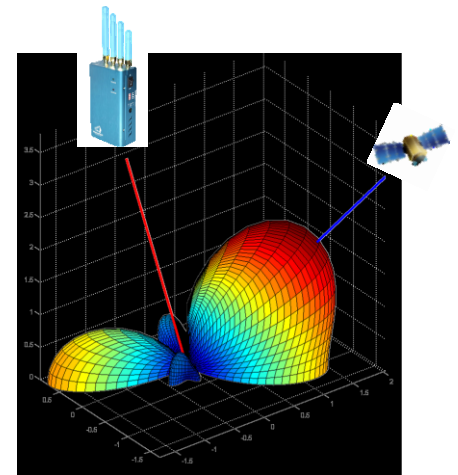
- The classic solution to jamming, is the controlled radiation pattern antenna (CRPA).
- Removes interference based on direction of arrival.



Defeating single jammer

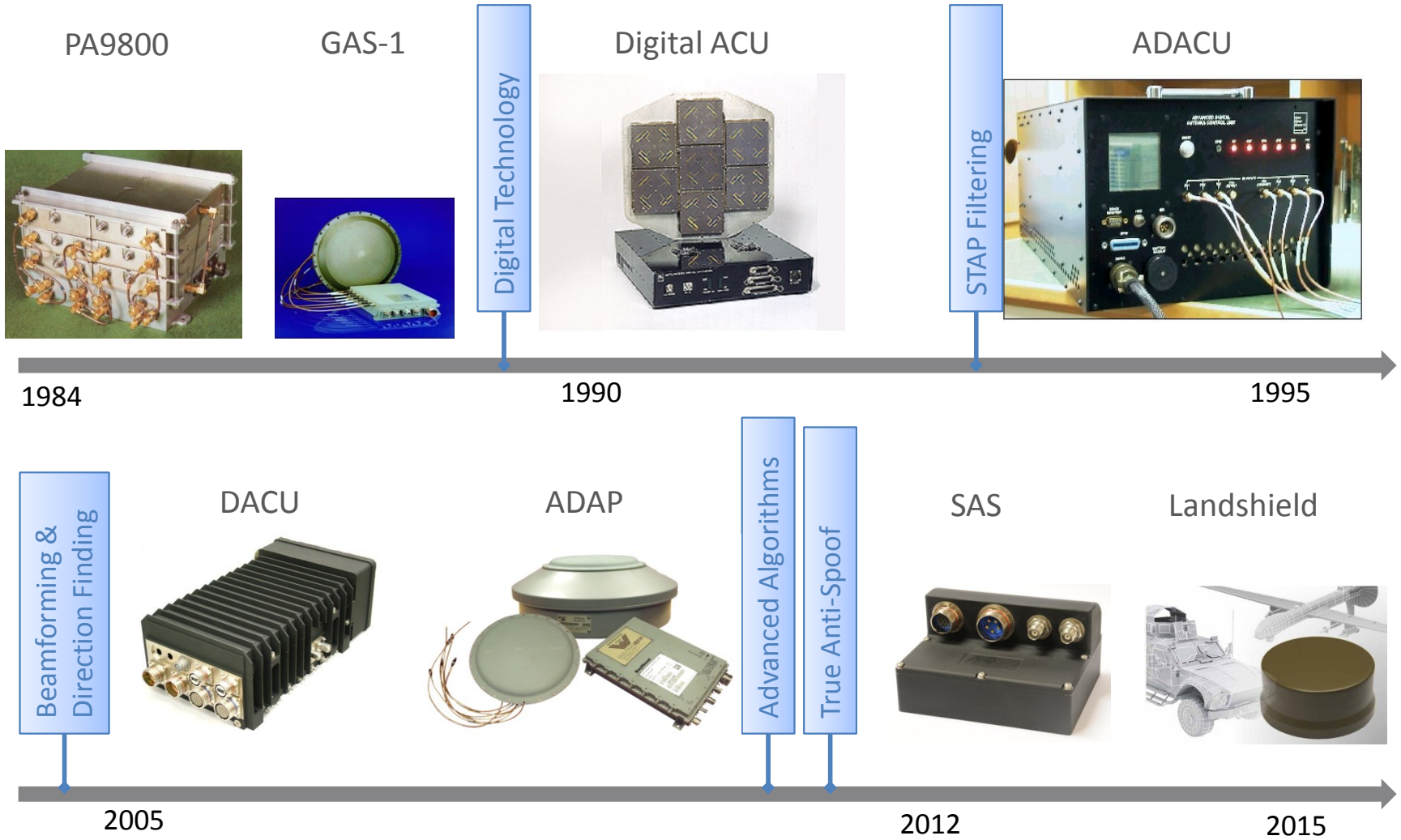


Defeating three jammers



**Improving satellite signal
by beamforming**

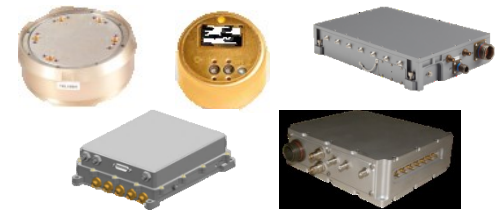
Anti-Jam Timeline: 1984 to 2017



Lot's of anti-jam products on the market...



Raytheon



Rockwell Collins



NovAtel

Plus Mayflower, Cobham, BAE,
Thales, Harris, Lockheed, L-3, and
others...

Example of state-of-the-art in 2017

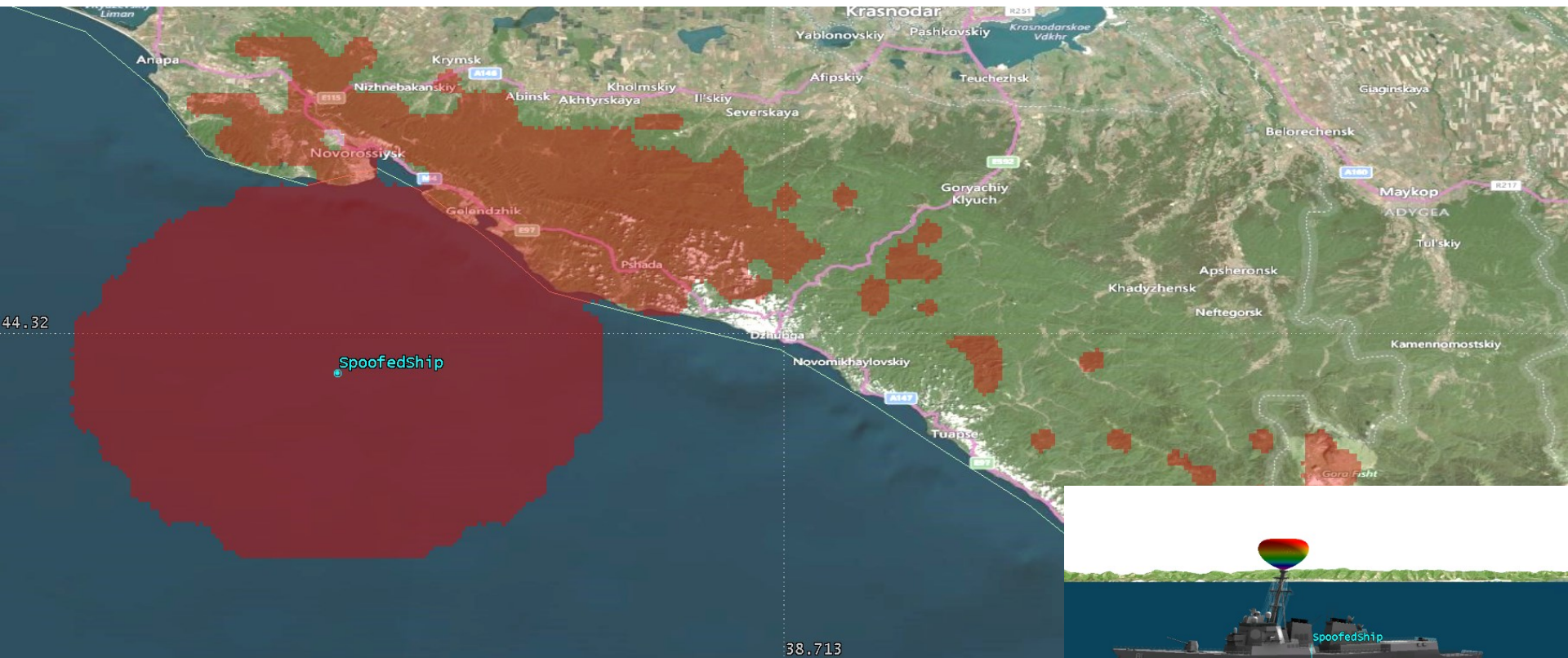
- Physically small
- Anti-jam (L1 & L2, M-code ready)
- True anti-spoofing (of GPS and Galileo open codes)
- Direction-finding of jammers and spoofers



Landshield
(Raytheon UK)

The current state of spoofing?

- Recent incidents around Russia show that large-scale spoofing is a reality.



Spoofting a receiver

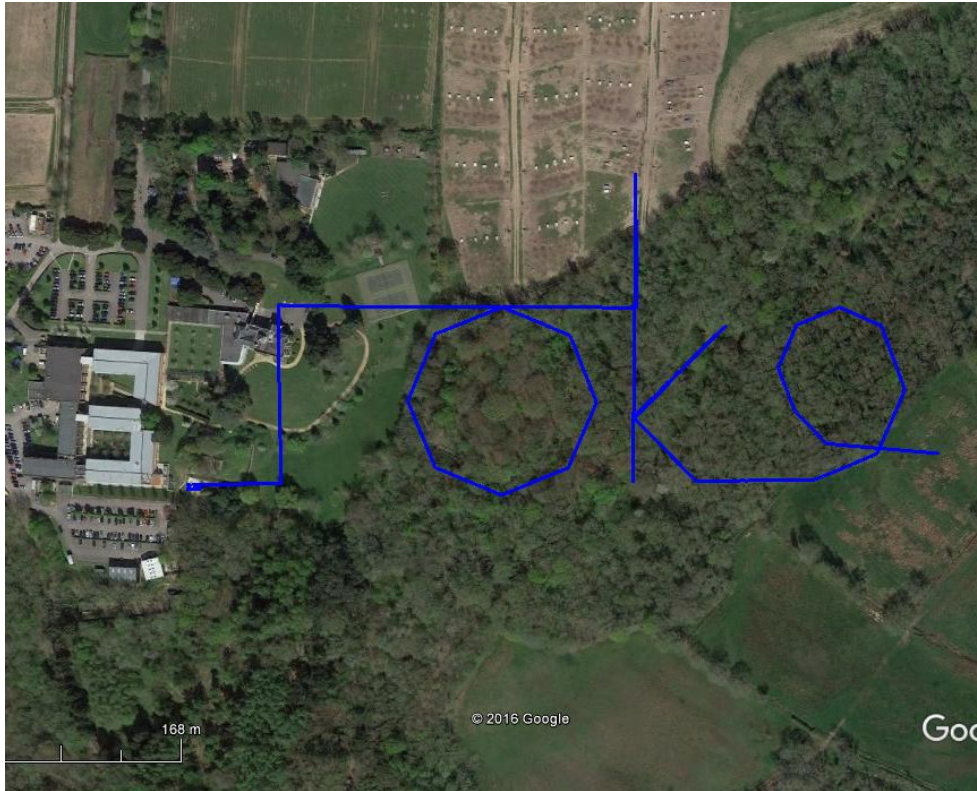


uBlox receiver spoofed without trouble

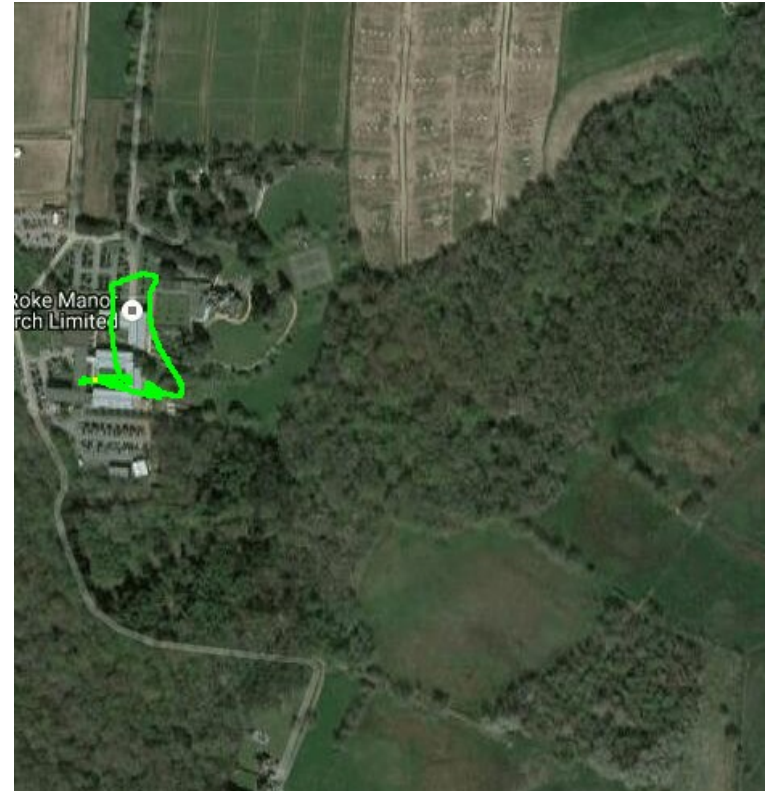


Conventional adaptive antenna does not help

Spooing and anti-spoofing a receiver



**VectorNav 300 is also spoofed,
despite its additional inertial
sensors**



**Adaptive antenna with anti-spoof
defeats spoofing attack**

(once anti-spoof is enabled, position
drifts back to correct location)

Anti-spoofing: user information

Spoof detected

Spoof satellite information

Anti Spoof

Spoof Detected: Detected

No Sats Tracked: 8

Noise: 49.852dB

DF Confidence: 94.5% (HF2)

DF Azimuth: 104.1 Degr (H4A)

DF Elevation: 52 Degr (H2C)

| Track Channel | SV | Doppler (Dec) | Aquisitions | State | Locked | C/No (dB) | Carrier (Hz) | Code (Hz) |
|---------------|----|---------------|-------------|-------------|--------|-----------|--------------|------------|
| 1 | 3 | 8 | 3 | Tracking | Green | 40.9 | 5132.02 | 1022995.00 |
| 2 | 1 | 5 | 1 | Tracking | Red | 41.8 | 2773.01 | 1023013.00 |
| 3 | 10 | -7 | 0 | Acquisition | Red | 0.0 | -4668.97 | 1023005.00 |
| 4 | 8 | 0 | 1 | Tracking | Green | 39.8 | -28.98 | 1022974.00 |
| 5 | 11 | 2 | 1 | Tracking | Green | 41.3 | 1328.03 | 1023005.00 |
| 6 | 9 | -9 | 0 | Acquisition | Red | 0.0 | -6003.00 | 1023005.00 |
| 7 | 23 | 13 | 2 | Tracking | Green | 43.6 | 7852.03 | 1023006.00 |
| 8 | 32 | 3 | 1 | Tracking | Green | 41.0 | 1009.03 | 1023013.00 |
| 9 | 22 | 8 | 1 | Tracking | Green | 44.9 | 4266.04 | 1022988.00 |
| 10 | 12 | -4 | 1 | Acquisition | Red | 0.0 | -2667.97 | 1023005.00 |
| 11 | 28 | 8 | 2 | Acquisition | Red | 0.0 | 5336.02 | 1023005.00 |
| 12 | 19 | 13 | 2 | Tracking | Green | 43.7 | 7538.03 | 1023022.00 |

Continuous Reading Single Read Save to File

But what about non-military applications?

Commonly-held views are that technology is:

- Classified
- Export-controlled
- Expensive

Classification

Recent examples are often UNCLASSIFIED.

Export

Typically free to export to 'sensible' countries.

Price

Some CRPAs have sold for less than \$500.

These are **not** blockers to commercial adoption of anti-jam technology

Anti-Jam for Civilian Applications

- Civilian and critical infrastructure applications have different requirements, compared to defense.



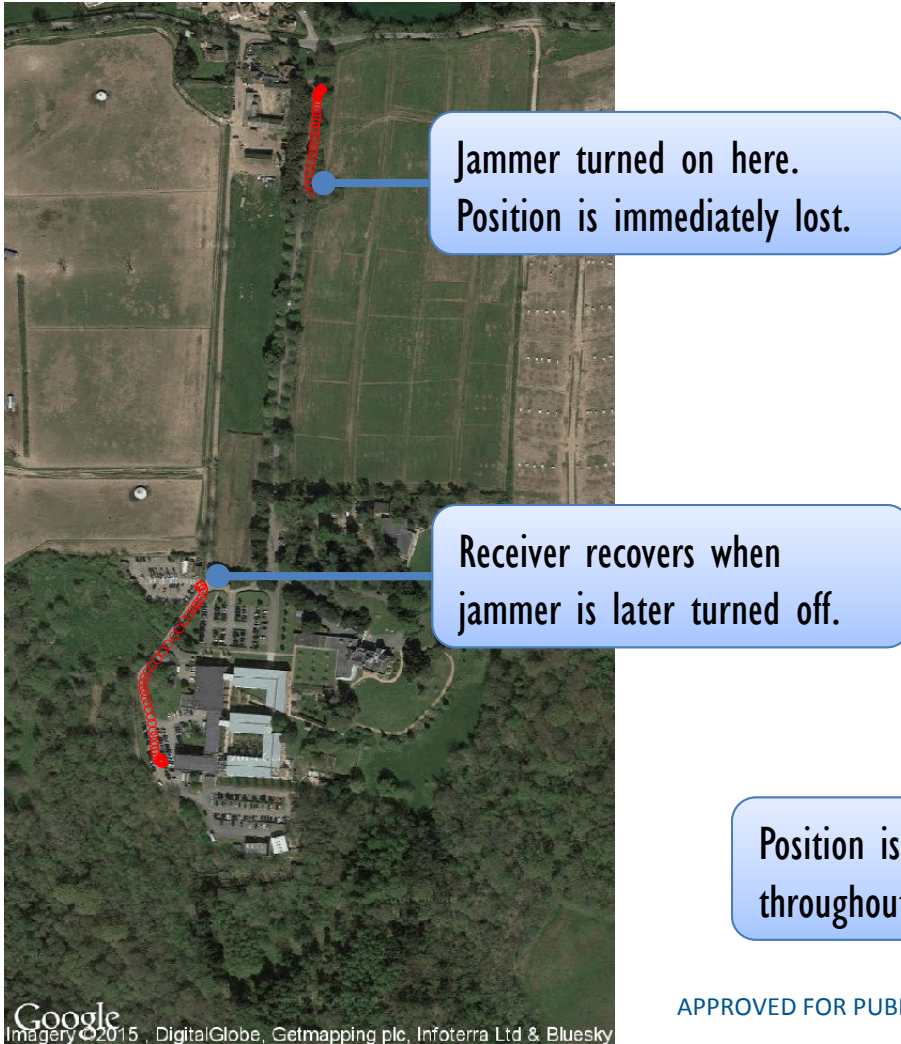
'Helium' antenna:
anti-jam for timing
receivers



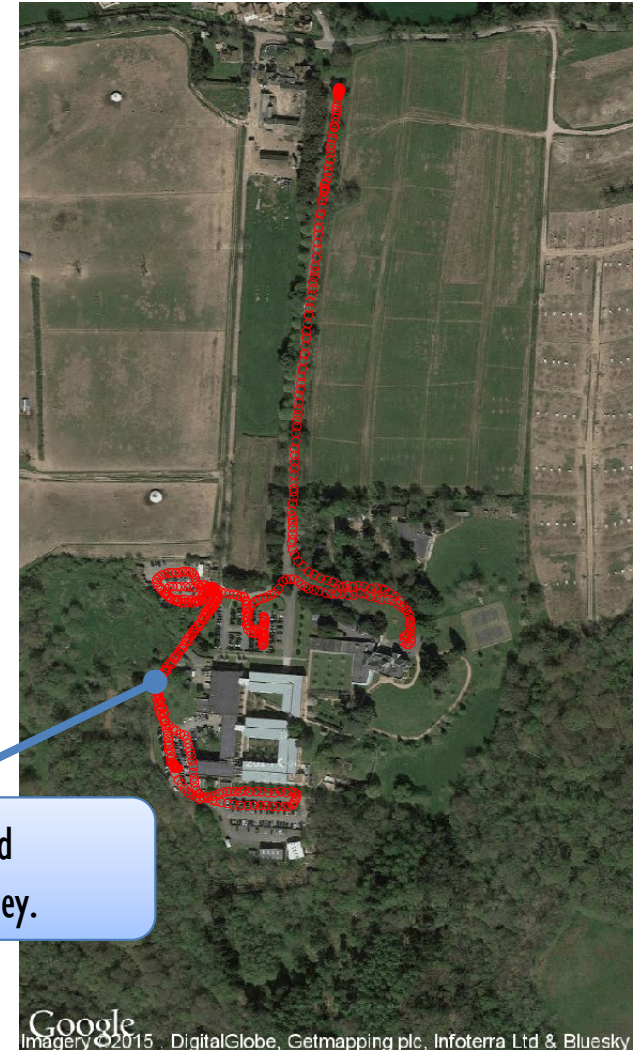
Ultra-low SWAP
mass-market anti-jam

Anti-jam trials in a car

Car operating a cigarette lighter jammer



Same car, also fitted with civilian anti-jam unit



Concluding Thoughts

- The world is in a good position, from a technology perspective.
- The technology exists to:
 - Detect and characterise interference (including spoofing)
 - Rapidly and precisely locate multiple interferers (including spoofing)
 - Mitigate interference (including spoofing)
- In the civilian domain, the problem is actually *market demand*.
- Significant uptake of protection technology will only occur if:
 - There is massive financial loss, or
 - There is legislation to force adoption