

Both the FAA and DoD are examining the vulnerability of GPS and our dependence on this "stealth" utility. So: ***How vulnerable is GPS?***

In discussions with a senior official last week, he expressed shock to find there is an perception in certain quarters that GPS vulnerability is so great, that DoD must abandon it and find an alternative.

Potential PNTAB Focus Item

- 3. ***Assess the vulnerability of GPS*** and what ***actions*** can/should be ***taken to reduce vulnerability and insure GPS availability?***

Note: Vulnerability means GPS is **not available** for **truthfully** determining position

Three Essential Attributes for any GNSS: the Three A's.



- **Availability** (Metric- **minutes of unavailability per day**) **Drivers:**
 - Satellite Geometry
 - Clear and truthful Reception
- **Affordability** – (Metrics: 1. Total Amortized ***cost per satellite-year*** [on orbit], 2. Cost of User Equipment [with req. interference resistance])
Drivers:
 - Cost of Satellite (driven by complexity and SWAP)
 - Cost of Booster and Satellites/Booster
 - Satellite Lifetime
- **Accuracy** – (Metrics: 1. **PNT 2σ accuracy** , 2. **Inaccuracy “bound”** (3 or 4σ), 3. “Integrity” - Probability that PNT Safety of Life value [10^{-7} ?] is exceeded)
Drivers:
 - Satellite Geometry
 - Ranging Accuracy

How vulnerable is GPS and what actions can/should be taken to reduce that vulnerability?

- **Availability** (Metric- *minutes of unavailability per day*)

Major Drivers:

– Satellite Geometry

- For sky-impaired, studies show 30+X are needed



– Clear *and truthful* Reception – **Threats:**

- Inadvertent interference – natural and human-made

- 
- **Deliberate interference** – Jamming and Spoofing

- Authorized Interference – Too powerful nearby signals

Deliberate interference – Jamming and Spoofing

- **Pre-action - Legal/Law Enforcement:**
 - Deterrence – Enact stiff laws, well publicized, international cooperation
 - Prevention – shutting down web sales of Jammers

What are the penalties for using GPS jammers in Australia?

offences under *Radiocommunications Act 1992*

- **Operation or supply of prohibited device - *two years* imprisonment or *\$255,000* —section 189**
- Causing interference likely to **prejudice the safe operation of vessels or aircraft - *five years* imprisonment or *\$850,000* —section 192**
- Causing interference to **rescue and emergency call service organisations - *five years* imprisonment or *\$850,000* —section 193**

Deliberate interference – Jamming and Spoofing

- **Re-actions when interference/spoofing**

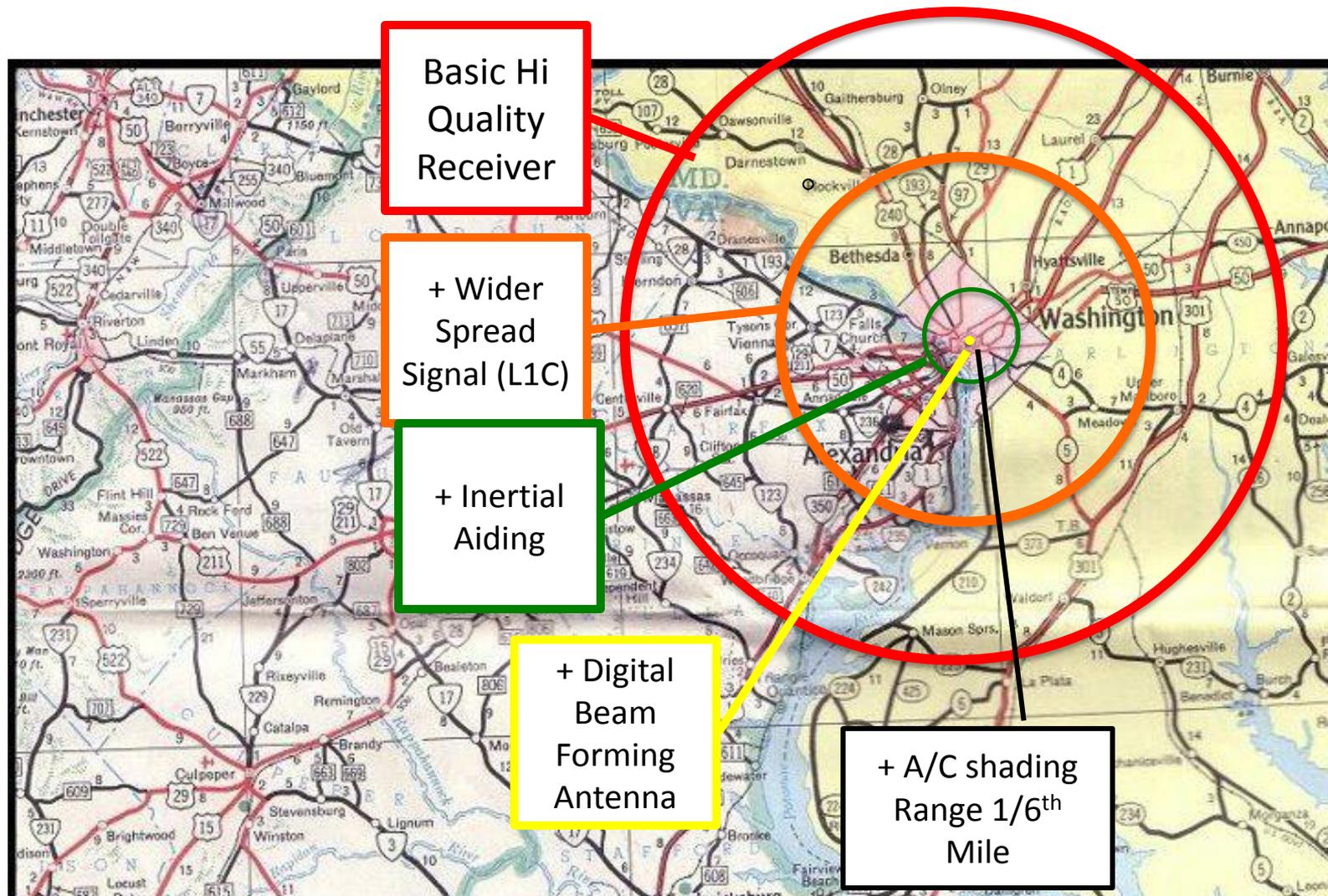
 - OCCURS - DOD/DHS/FCC/FBI:**

 - Detection – Timely knowledge of interference
 - Identification - Rapid pinpointing of interference source
 - Elimination – Physical suppression and removal of device
 - Prosecution – Application of the law
 - Apply Australian type Penalties for possession and use

- **Mitigations**

 - UE toughening -
 - All GNSS signal receivers (with vector feature)
 - Increasing Jam resistance
 - Backup PNT Sources
 - eLoran
 - Modernized DMEs





Effective Areas of **1KW** Jammer Against GPS A/J “Nibbles”

So...

- Under some circumstances, GPS may be Vulnerable
- Steps are **available and well-known** to greatly reduce vulnerability
- Need further Board Study
 - Likelihood of Problem
 - Impact of Problem
 - Mitigations – short term and long term
- And Promulgate credible assessment

Focus Items

- 1. What is a supportable **measure of the economic value** of GPS to the Nation? (As a sub, if our new economic study comes up with credible estimates, what can we do to help promulgate that value?)
- 2. There is enormous pressure on DoD (and the Air Force) to reduce the budget. What steps might the board recommend to insure GPS viability in the coming years?
- 3. Both the FAA and DoD are examining the vulnerability of GPS and our dependence on this "stealth" utility. So: **How vulnerable is GPS** and what **actions** can/should be **taken to reduce that vulnerability**? In discussions with General Shelton last week, he was shocked to find there is an attitude that GPS vulnerability is so great, that DoD must abandon it and find an alternative. I personally have advocated a backup for PNT (eLoran and/or advanced DME), but I think this question should be more deeply examined.
-