GPS Jamming Detection & Geolocation

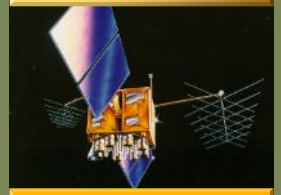
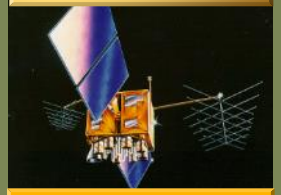
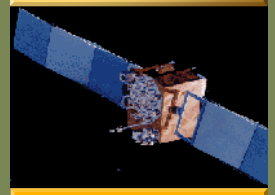
Joe Rolli

March 2015

Exelis innovation across the GPS constellation

On-orbit reprogrammability | RAFS | M-code | Interplex Modulation | Upgradeable architecture

Blk II Triplexer | AutoNav | Flex Power | TKS | NDU M code approach | DWG | Hi-power M-code

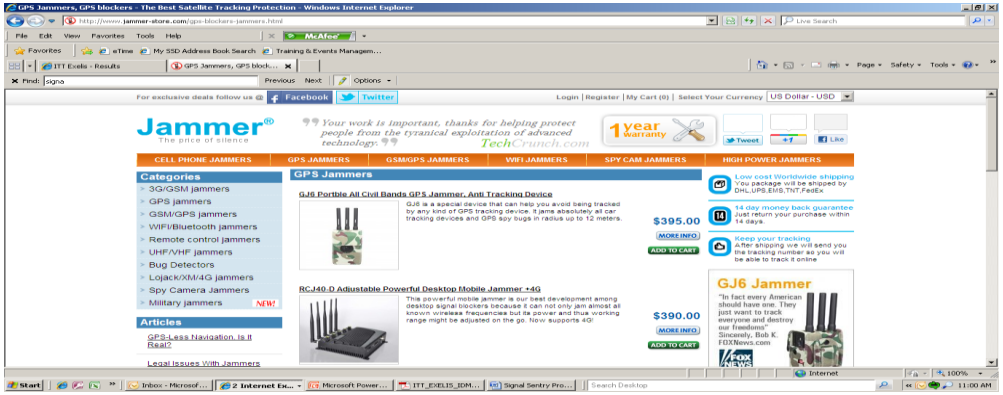
1974-1983	1983-1988	1988-1999	2000-Present	2003-Present	2008-Present
					
ROCKWELL	ROCKWELL	LOCKHEED MARTIN	LOCKHEED MARTIN	BOEING	LOCKHEED MARTIN
Block I	*Block II/IIA*	*Block IIR*	*Block IIR-M*	*Block IIF*	*Block III*
12 Flight Payloads	28 Flight Payloads	13 Flight Payloads	8 Flight Payloads	12 Flight Payloads	32 Flight Payloads
GPS Signals	**GPS Transmitters**	**Fully Integrated GPS Payload**	**GPS Modernization**	**GPS IIF**	**GPS III**
• Code Generators • L1 Transmitter • L2 Transmitter	• L1 Transmitter • L2 Tramsmitter • Triplexer	• On-Orbit Reprogrammability • Crosslink Ranging • Self Navigation (AutoNav) • Improved Accuracy (1m) • Improved Time Keeping • Improved Security	• On-Orbit Signal Structure Changes • Enhanced Signal Security Per NSA • High Power GaAs Transmitters • New High Power Military Unique Signals	• Flexible RF Power • High Power GaAs Transmitters	• DWG capability insertion • New International Signal (L1C) • High power/flexible power • Anti-Jam Military Signals • Hi-gain M-code capability

Exelis has developed and Implemented navigation signals for every generation of GPS

Exelis has been at the forefront of GPS innovations since the 1970s

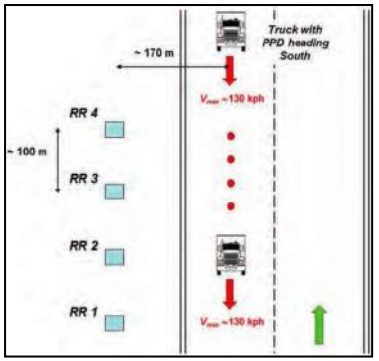
Jamming

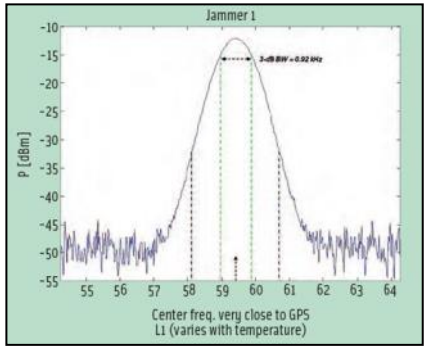
- GPS jamming does not allow receivers to lock onto the GPS signal
- GPS susceptible to outages due to intentional & unintentional jamming
- A small jammer can disrupt the GPS signal for a mile or more
- People jam because they are smuggling, stealing or trying to escape tracking
- Availability of low-cost GPS jamming devices has increased the risk

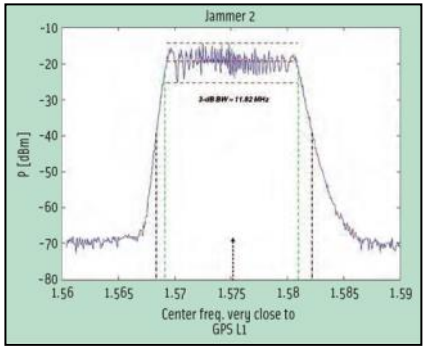


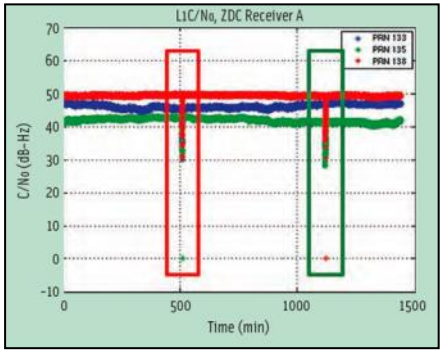
The Risk is Real – Jamming at Newark Airport (Nov-09)

- November 2009
- Ground-based Augmentation Systems (GBAS) Jammed
- Took 3 months to find the source









Source:
http://www.insidegnss.com/node/2976

PNT Advisory Board (Nov-10)

Summary: The United States is now critically dependent on GPS. For example, cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System (NEXGEN) cannot function without it. Yet we find increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations.

Most alarming, the very recent web availability of small GPS-Jammers suggests the problem will get worse. These so-called *personal protection devices (PPDs) as well as other, readily available,* more powerful devices can deliberately jam the Global Positioning System (GPS) signal over tens of square miles. They also can be devastating to the other, new foreign satellite navigation systems being deployed worldwide. PPDs are illegal to operate, but many versions are available (for as little as $30) from foreign manufacturers over the Internet. The simplest models plug in to a cigarette lighter and prevent all GPS reception within a line of sight range of 5 to 10 miles. Current penalty for operation is simply that the device is confiscated. We currently lack sufficient capabilities to locate and mitigate GPS jamming. It literally took months to locate such a device that was interfering with a new GPS based landing system being installed at Newark Airport, NJ.

The Risk is Real: Jamming at Newark Airport (Aug-12)

- August 4, 2012: FCC fines man $32K
- For illegal GPS Devices that disrupted Newark Liberty International Airport
- The man claimed he was simply trying to hide from his employer

Thieves Use GPS Jamming to Steal Pharma Cargo (July -14)

Pharmaceutical Cargo Security Collation (PCSC)

http://www.securingindustry.com/pharmaceuticals/pharma-cargo-thieves-start-to-deploy-jamming-technology/s40/a2103/#.VDX8O_ldWSo

Are GPS jammers the next frontier in cargo theft?

http://m.landlinemag.com/Story.aspx?StoryID=27451#.VDXZhPjD8uw

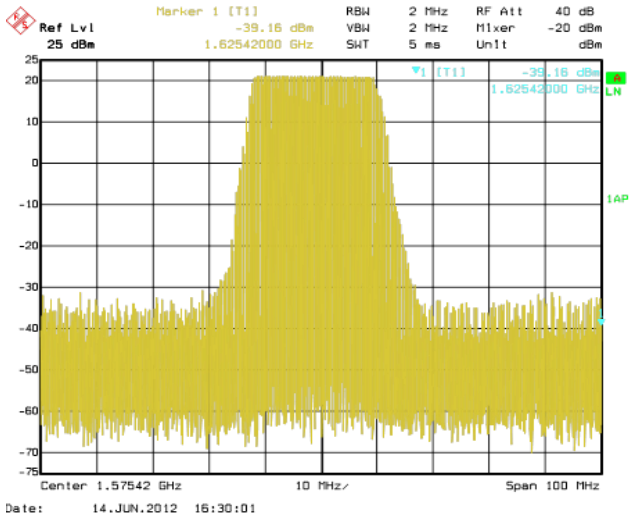
Jammer Description

1.0 Jammer Description

There were two Jammers utilized during the trials, 150mW and .5W. The jammers that were used to disrupt the GPS L1CA code that operates at 1575.42 MHz. The following Information below characterizes each jammer.

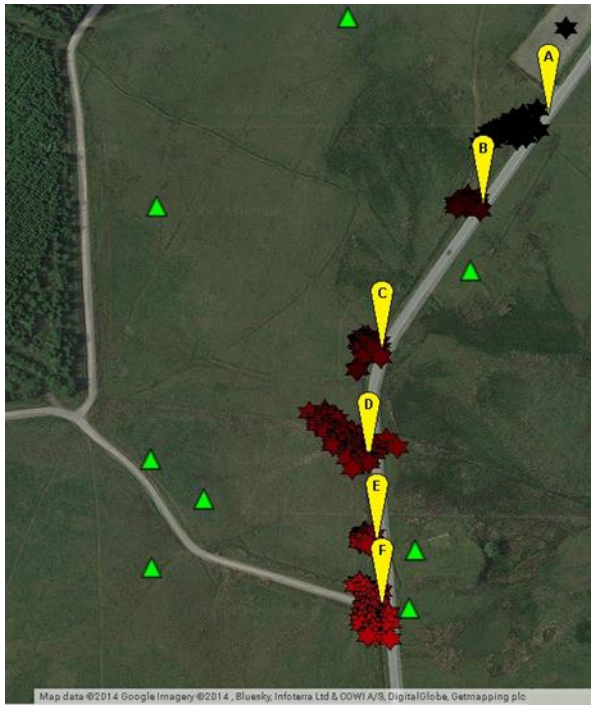
1.1 150mW Jammer

The physical form of the jammer and the waveform for the jammer is shown in Figure 3-1.



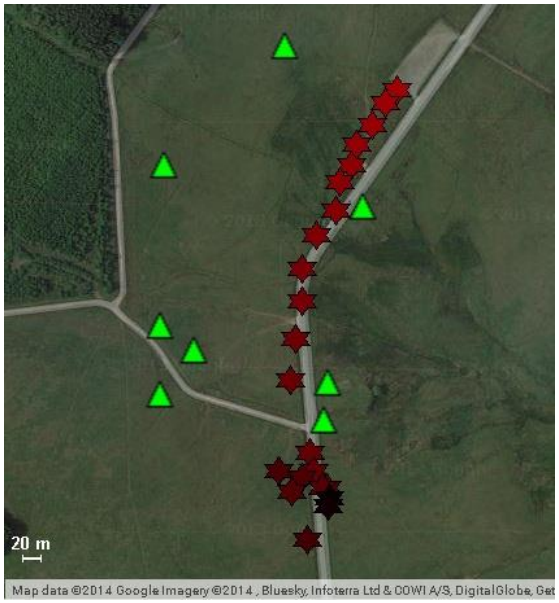
Control Test Aug 2014 Sennybridge Test Range in the UK

Stationary Test



Waypoint	Accuracy Error (m)	
A	39.7	
B	13.0	
C	10.8	
D	10.7	
E	12.1	

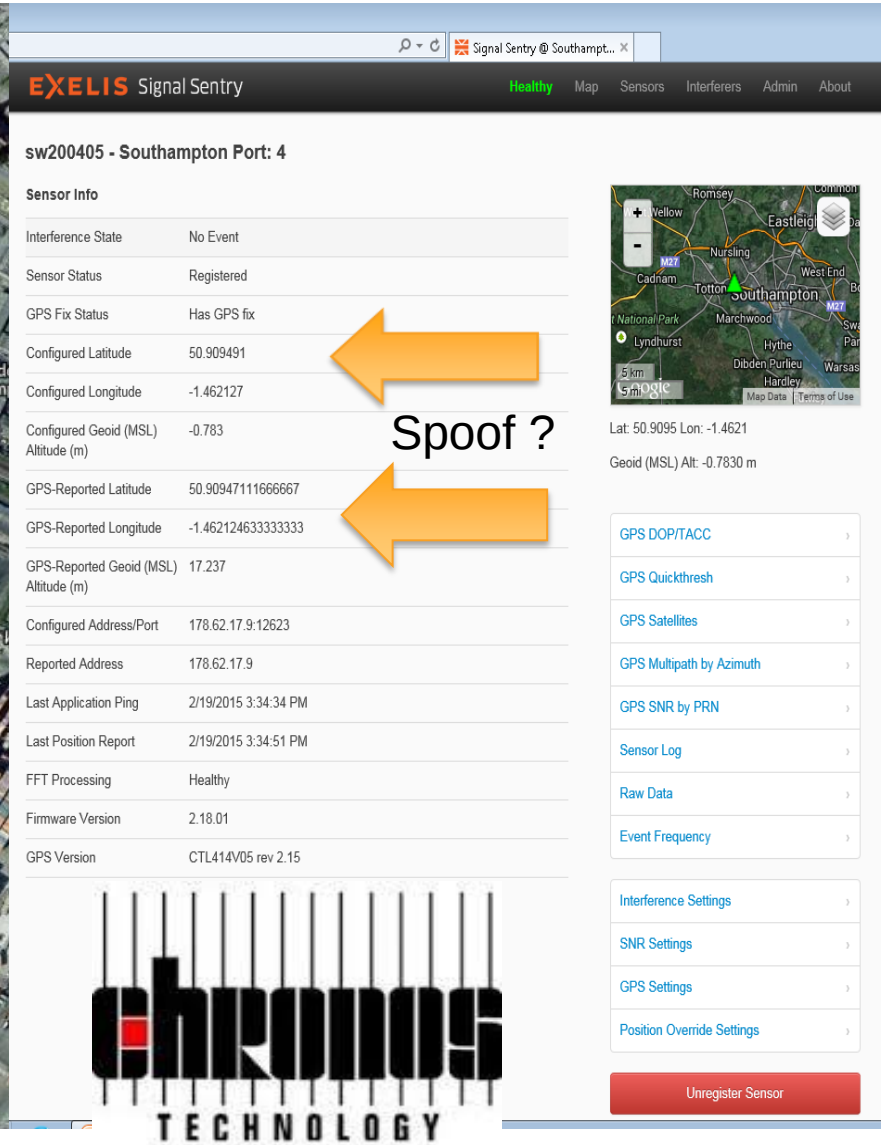
Car moving 40 MPH



Difficult to measure accuracy of a moving car

Test Sponsored by the UK MOD

Dec 2015 First Install At Southampton Port UK Chronos VAR



PNT Advisory Board Specific Recommendations

1. **National Focus**
   - GPS should be formally declared critical infrastructure by Executive Branch and managed as such by DHS.
2. **National Alerting and Pinpointing Interference Locations** 
   - The National Executive Committee should establish and sponsor a National GPS Interference Locating, Reporting, and Elimination System; coordinating and expanding on the resources of several Departments.
3. **Shutting Down and Prosecuting Interferers**
   - Legal and Law Enforcement actions. The National Executive Committee should examine whether or not they should sponsor Legislation in Congress that addresses interference to GPS that provides substantial fines and jail time for both possession and use of GPS jammers.
4. **Hardening GPS Receivers and Antennas**
   - Government should foster and help to stimulate Manufacturers to speed up the development and offering of interference resistant GPS receivers, especially for safety-of-life applications such as commercial air and maritime.
5. **Fund a National back-up capability to insure continuity of PNT Operations**
   - We strongly recommend that the previously announced decision (to deploy eLoran as the primary Alternate PNT) should be reconfirmed and quickly implemented. We support the FAA's efforts to provide Alternate PNT options that can provide a robust backup to GPS and deter malicious interference.