Vulnerability Threats to the Future of GNSS

Andrew Dempster
The Big Picture

- GNSS is now critical infrastructure
- GNSS are weak and hence vulnerable
- Incentive has been created for civilian jamming
- The once in 200 year Carrington event was 155 years ago…
Critical Infrastructure

http://www.insidegnss.com/node/3108
**CI Sectors**

- 15/18 use GPS timing
- +3 for positioning?

<table>
<thead>
<tr>
<th>CIKR Sector</th>
<th>Uses GPS Timing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Sector</td>
<td>X</td>
</tr>
<tr>
<td>Emergency Services Sector</td>
<td>X</td>
</tr>
<tr>
<td>Information Technology Sector</td>
<td>X</td>
</tr>
<tr>
<td>Banking &amp; Finance Sector</td>
<td>X</td>
</tr>
<tr>
<td>Healthcare &amp; Public Health Sector</td>
<td>X</td>
</tr>
<tr>
<td>Energy/Electric Power and Oil &amp; Natural Gas SubSector</td>
<td>X</td>
</tr>
<tr>
<td>Nuclear Sector</td>
<td>X</td>
</tr>
<tr>
<td>Dams Sector</td>
<td>X</td>
</tr>
<tr>
<td>Chemical Sector</td>
<td>X</td>
</tr>
<tr>
<td>Critical Manufacturing</td>
<td>X</td>
</tr>
<tr>
<td>Defense Industrial Base Sectors</td>
<td>X</td>
</tr>
<tr>
<td>Postal &amp; Shipping Sector</td>
<td>X</td>
</tr>
<tr>
<td>Transportation Sector</td>
<td>X</td>
</tr>
<tr>
<td>Government Facilities Sector</td>
<td>X</td>
</tr>
<tr>
<td>Commercial Facilities Sector</td>
<td>X</td>
</tr>
<tr>
<td>National Monuments and Icons Sector</td>
<td></td>
</tr>
<tr>
<td>Agriculture and Food Sector</td>
<td></td>
</tr>
<tr>
<td>Water and Wastewater Sector</td>
<td></td>
</tr>
</tbody>
</table>
President Obama raises infrastructure needs during 2013 State of the Union address on February 13.
White House photo (Click image to enlarge.)

White House Moves to Harden Infrastructure against GPS Disruption

"GPS a "cross-sector dependency""

Latest News

Dee Ann Divis
May 13, 2013

By Mike Gruss | Nov. 25, 2013

WASHINGTON — As jamming and disruptions to the nation’s positioning, navigation and timing satellites become more commonplace, the federal agency in charge of coordinating a national effort to protect critical infrastructure cannot ensure that “essential” operations would continue during an outage, according to a new report.

GPS “has become an invisible utility that users do not realize underpins their applications, leaving sectors potentially vulnerable to GPS disruptions,” a Nov. 6 report from the Government Accountability Office (GAO) read.

Industry officials have said the proliferation of GPS jamming devices is creating a market for countermeasures, both in the defense and commercial sectors. In a speech at the annual Air Force Association conference Sept. 17, Gen. William Shelton, commander of Air Force Space Command, which operates the 30-plus satellite GPS constellation, highlighted jamming as an increasingly common problem.

But too often, the GAO report said, GPS outages are viewed as “low risk.”
The “Casual terrorist”

• Courier driver jams his van’s GPS to visit his girlfriend near Newark Airport...
Melbourne cabbie fined over GPS jammer

Radio comms could be blocked in fight for passengers.

A Melbourne taxi driver has been fined $850 after pleading guilty to using a GPS jammer.

The Australian Communications and Media Authority (ACMA) — which regulates spectrum usage in Australia — noted the Magistrates Court conviction in a brief blog post today.

The conviction appears to be the result of a sting by the ACMA and Victorian Taxi Services Commission that was carried out at Melbourne city and airport taxi ranks in early-to-mid 2013.

The two-stage joint operation saw ACMA inspectors set up a spectrum analyser near taxi ranks and speak to around 300 drivers about the issue of GPS jamming.

Two drivers were reportedly charged with breaking radiocommunications laws. Both were due to face court last month. Other drivers were "reprimanded" or "given their marching orders", according a Herald Sun report.

Allegations of jammer use among Melbourne cabbies were aired back in 2012.
31 March 2011, 7.02am AEST

GPS jamming could make you a casual terrorist

AUTHOR
Andrew Dempster
Professor, School of Surveying & Spatial Information Systems at University of New South Wales

DISCLOSURE STATEMENT
Andrew Dempster receives funding from the ARC to investigate geolocating jamming sources.
Threats

- “Personal Privacy Devices”
- Transmitters at nearby frequencies
- Intentional regional jamming
2011: LightSquared: the big (only?) news

LIGHTSQUARED VS. GPS
LightSquared Promises GPS Mitigation Plan for Skeptical House Members
[GNSS SIGNALS exclusive] Would-be cellular broadband company LightSquared promised a Congressional subcommittee on June 23 that it would scale back its proposed wireless system and help pay to find a way to mitigate the network's adverse effects on users of the Global Positioning System. [more]

$96 Billion Annual GPS Commercial Losses from LightSquared Interference?
Interference from LightSquared transmitters could cost manufacturers and users of commercial GPS technology — not including consumers or aviation users — up to $96 billion in annual losses, according to a study by a Washington, D.C.-based economic consulting firm presented on June 22. [more]

Senate Proposals for GPS Receiver Standards Won’t Solve LightSquared Issue
[GNSS SIGNALS exclusive] The U.S. Senate is considering mandated standards for GPS receiver designs that could withstand interference from services using nearby frequencies. The hope: more users packed into swaths of the spectrum. The fear: more expense, and it still wouldn’t solve the LightSquared problem. [more]
Why is it a Problem?

**Figure 2.** Band Pass Filter Diagram. From Deere: LightSquared Interference to GPS and StarFire, May 26, 2011, filing to Federal Communications Commission.
Battle Won, War Goes On...
Television Stations

- SBS, Artarmon 527.25 MHz
Global L-band interference
• From SMOS satellite 1400-1427 MHz
Those North Koreans...

<table>
<thead>
<tr>
<th>Dates</th>
<th>Jammer locations</th>
<th>Affected areas</th>
<th>GPS disruptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 23-26, 2010 (4 days)</td>
<td>Kaesong</td>
<td>Gimpo, Paju, etc.</td>
<td>181 cell towers, 15 airplanes, 1 battle ship</td>
</tr>
<tr>
<td>Mar 4-14, 2011 (11 days)</td>
<td>Kaesong, Mt. Kumgang</td>
<td>Gimpo, Paju, Gangwon, etc.</td>
<td>145 cell towers, 106 airplanes, 10 ships</td>
</tr>
<tr>
<td>Apr 28 – May 13, 2012 (16 days)</td>
<td>Kaesong</td>
<td>Gimpo, Paju, etc.</td>
<td>1,016 airplanes, 254 ships</td>
</tr>
</tbody>
</table>

[The Central Radio Management Office, South Korea]

http://www.insidegnss.com/node/3982

GNSS Futures, UNSW, 7-8 July 2014
Remedies
Detection?

Radar gun spots vehicles with illegal GPS jammers

17:33 02 August 2013 by Paul Marks
For similar stories, visit the Crime and Forensics Topic Guide

The battle against truckers and motorists who jam GPS signals has moved up a gear. A new handheld radar can pinpoint which vehicles are illegally using the jammers to stop their bosses from monitoring where they drive or to dodge automatic tolls on motorways.

Used just like a speed gun, a police or customs officer would train the iPad sized gadget, made by Chronos Technology of Lydbrook, UK, on queues of traffic – or even on people walking down the street.

The device is needed because a £50 jammer, which can be bought online, can cause widespread GPS outages thanks to the low power of the GPS satellite signal.

Until now, says navigation engineer Ian Colts at Chronos, a number of devices have been available to law enforcement officers who want to detect jammers. But existing detectors can only detect the presence of a jammer, not find out...
Geolocation

Prototype collinear antenna array

AOA: 3.3m
TDOA: 1.7m
GPS Jammer Fined $32,000

A New Jersey man who didn't want his boss following his every move has lost his job and had the book thrown at him by the FCC because the inexpensive ($68 and up) GPS jammer he carried in his truck shut down an experimental, high-tech, multimillion-dollar navigation system at Newark Liberty Airport. Gary Bojczak was fined $31,875 by the FCC after admitting that he carried the device, which is readily available for sale on the Internet, so he could disable the GPS transmitter on the pickup truck he drove for engineering company Ticon. He apparently didn't want his bosses to know his whereabouts when he was near the airport and his little jammer brought down a Ground Based Augmentation System (GBAS) being tested by Honeywell.

GBAS is designed to provide guidance for instrument approaches and departures with an accuracy of one meter. It can, when it’s not being jammed by what looks like a deck of cards with one or more antennae sticking out of it (some simply plug into a vehicle power port), provide precision necessary for Cat III approaches. When the system experienced "interference" the FCC went looking for the culprit using "direction finding techniques" and confronted Bojczak, who readily admitted to using the jammer. Ironically, GPS jamming detectors are also available from sites that offer the jammers but it's not clear where the FCC got its gear. However they found him, they showed no mercy on the privacy-seeking truck driver. While it's normal, according to electronics industry attorney Chip Yorkgitis, for those whose electronic experiments interfere with others using the same area of frequency to get off with a warning, the FCC skipped the warning and fined Bojczak heavily. Yorkgitis said that if the heavy fine isn't enough to deter others from using the apparently common devices, criminal charges are the next option.

FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS

Jamming events continue — an average of five per day at EWR

Glen Gibbons
August 30, 2015

The Federal Communications Commission (FCC) has proposed a hefty fine for a New Jersey truck driver whose alleged use of a GPS jammer caused harmful interference to the new ground-based augmentation system (GBAS) at Newark Liberty International Airport (EWR).
Illegal mobile phone and GPS jammer crackdown by regulator yields results

July 17, 2013

Ben Grubb
Deputy Technology editor

View more articles from Ben Grubb
Follow Ben on Twitter Follow Ben on Google+ Email Ben

Illegal mobile phone and GPS jammer crackdown by regulator yields results

FOR IMMEDIATE RELEASE:
October 5, 2011

WASHINGTON, D.C. – The FCC Enforcement Bureau has issued 20 enforcement actions against online retailers in 12 states for illegally marketing more than 200 uniquely-described models of cell phone jammers, GPS jammers, Wi-Fi jammers, and similar signal jamming devices. These devices have the
Backup Systems

**Inside GNSS**

**INSIDE GNSS NEWS**

**GPS Spoofing Experiment Knocks Ship off Course**

*University of Texas at Austin team repeats spoofing demonstration with a superyacht.*

**Latest News**

Dee Ann Divis  
July 31, 2013

**Share via:**  
Reddit | Technorati  
Twitter | Facebook

In a startling experiment a research team from the University of Texas successfully spoofed a ship’s GPS-based navigation system sending the 213-foot yacht hundreds of yards off course — without raising alarms or triggering a hint of the course change on the onboard monitors.

---

**PocketGPSWorld**

**GPS Speed Switch**

*www.gpsspeed.com.au*

No calibration required Switch settable.

**UK deploys eLoran to protect shipping against GPS jamming**

*Article by: Darren Griffin  
Date: 17 Jul 2013*

The spoofed route of the White Rose of Drachs was not detected on the ship’s navigation monitors. Photo courtesy of University of Texas at Austin (Click image to enlarge.)

**UK deploys eLoran to defend against GPS Jamming**

The UK will become the first country to deploy equipment to protect against the threat of GPS jamming.
The Owners are worried
And yet…

• “Joined-up government”?
New Foundation Formed to Pursue eLoran as Backup for GPS

Racing against the clock before Loran sites torn down

Operational cost would be "budget dust."

Dee Ann Divis
November 7, 2013
Inside GNSS, November/December 2013

Share via: Slackdot Technorati
Twitter Facebook

A new nonprofit has been launched to push for repurposing the United States' old C-Loran infrastructure to support a new system.

Nominal UK eLoran system design. General

House Committee Moves to Block Loran-C Teardowns

To preserve for possible use in GPS backup system

Enhanced Loran gets new backing.

Dee Ann Divis
February 14, 2014

Share via: Slackdot Technorati
Twitter Facebook

Lawmakers overseeing the Coast Guard approved language this week that would stop the agency from dismantling facilities needed for eLoran, a proposed system that has gained wider support.
Trends

• More reliant on GNSS
• Higher incidence of jamming
• Recognition of the problem:
  – US: Dept Homeland Security
  – US: Resilient Navigation and Timing Foundation
  – Aus: Trusted Information Sharing Network
Future

• Governments:
  – Legislate/ detect/ punish
  – Train experts
  – Maintain alternative infrastructure

• GNSS Designers:
  – Be ready for neighbouring frequency allocation
  – Design in interference detection, characterisation, location, mitigation
The End