SPACE-BASED POSITIONING
NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

Overview of Protecting, Toughening, and Augmenting the Use of GPS

24 April 2024

PTA

Today's PTA Agenda

- 10:30 to 11:30 PTA Overview
- 11:30 to 12:30 Lunch
- 12:30 to 1:45 Protect, with Board Discussion
- 1:45 to 2:00 Break
- 2:00 to 3:15 Toughen, with Board Discussion
- 3:15 to 3:30 Break
- 3:30 to 4:45 Augment, with Board Discussion
- 4:45 to 5:00 PTA Summary
- 5:00 to 6:00 Board Deliberations
- 6:00 Adjourn

PTA

GPS Provides Positioning, Navigation, and Timing (PNT) to Our Nation and the World

50+ Years of GPS Success

- GPS program inaugurated in 1973
- Visionary leadership, strong U.S. Government investment—from early concept, to system demonstration, to deployment, to sustainment, to modernization
- Ubiquitous PNT for billions of users and thousands of applications across the world
- Convergence of multiple technology advancements: signals, electronics, software
- Massive private investment, innovation, adoption in civil, commercial, mass public markets
- As of 2019, U.S. private sector has gained an estimated $1.4 trillion in economic benefits since private sector use began in the 1980s [1]
- No other PNT technology provides the accuracy, availability, integrity, wide service region, day/night and all-weather capability, and low cost to users
- Widespread use and dependence on GPS
  - Most important civil use is for critical infrastructure

PTA

1. Economic Benefits of the Global Positioning System to the U.S. Private Sector Study | NIST

GPS Needs Renewed Attention

- Widespread dependence on GPS makes its vulnerabilities a risk in critical infrastructure and other applications
- GPS civil user devices have typically been developed and tested assuming clean spectrum and no malevolent actors
- Other technologies, especially mobile broadband communications, seek to use frequencies adjacent to those where GPS signals operate, causing interference to high-accuracy and safety-of-life users
- Other nations have fielded their own versions of GPS, providing more features than GPS offers
- GPS modernization has been slow and expensive

Spectrum Management Concerns

REUTERS® World Business Markets Sustainability More My View

Technology

FCC approves Ligado plan to deploy mobile broadband network

By **David Shepardson**

April 20, 2020 12:59 PM EDT · Updated 4 years ago

WASHINGTON (Reuters) - The five-member Federal Communications Commission voted unanimously to approve an order to allow Ligado Networks to deploy a low-power nationwide 5 network despite objections from the U.S. Defense Department, other federal agencies and maj U.S. airlines.

The telecommunications regulator said on Monday the approval order included stringent conditions aimed at ensuring global positioning systems would not experience harmful interference.

Fierce Wireless Fierce Telecom Fierce Electronics Silverlinings Wireless/Telecom Events Broadband Expo Advertise About Us

FIERCE Wireless Wireless Private Wireless 5G Tech

5G

Pressure mounts on FCC to stop Ligado's L-Band plan

By **Julia King** · Jun 26, 2023 1:04pm

Ligado Networks Iridium FCC 5G spectrum

AVIATION TODAY

AVIONICS INTERNATIONAL

Avionics Vendor Directory | Search Subscribe

CONNECTED AVIATION INTELLIGENCE SUMMIT 2023

2023 Participating Companies 2023 Agenda Pricing Sponsorship Opportunities VISA Invitation Hotel & Travel

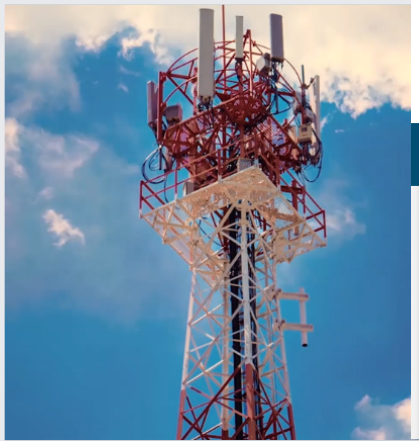
September 6-8, 2023 | Hilton City Center De

Aviation Stakeholders Tell Congress of Opposition to FCC Order on Ligado L-Band License

By **Frank Wolfe** | May 8, 2020

Send Feedback

5G, aviation, FCC, GPS, Ligado Networks



IG Inside GNSS

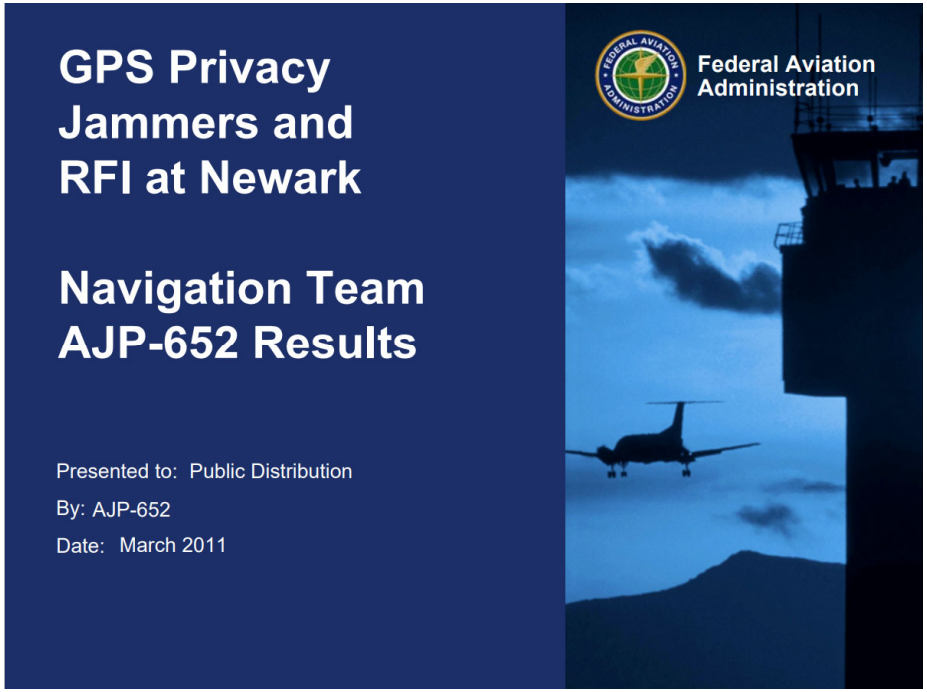
Global Navigation Satellite Systems Engineering, Policy, and Design

Home Applications Columnists Insider Subscribe Custom Con

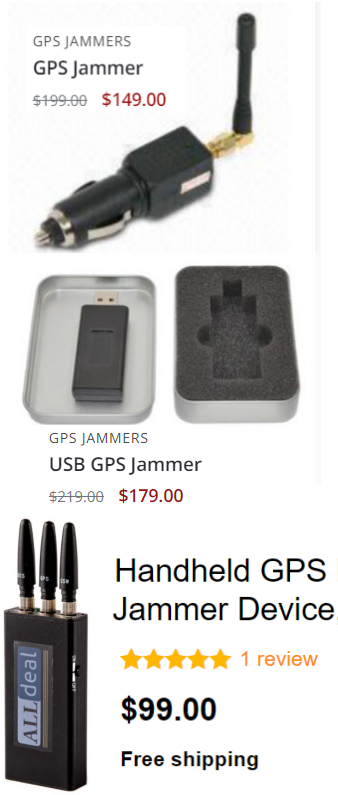
Pentagon Opposes Ligado's Wireless Network Proposal

November 21, 2019 By Dee Ann Divis

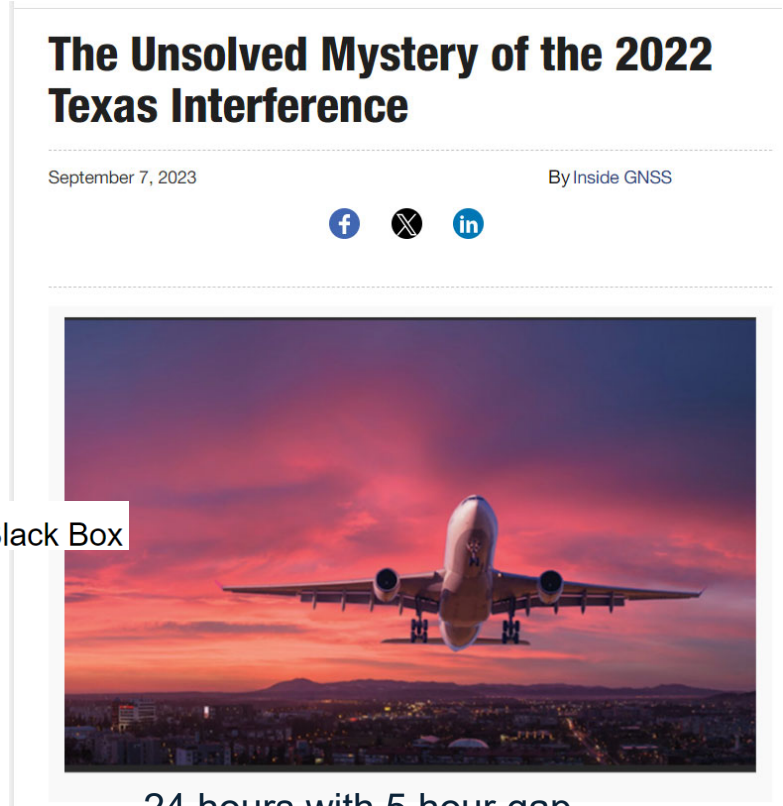
Interference Happens to GPS Reception in the U.S.



- Interference intermittently shut down GPS-based aid to navigation
- Six months to find and remove mobile source



- Personal privacy jammers easy to buy
- Can affect receivers more than 1 km away



24 hours with 5 hour gap
Caused runway closure
Source never identified

PTA

Finding and Removing Interference Sources Is a Challenge

GOVERNMENT REPORTS AND SUMMARIES LATEST FROM GAO
TRANSPORTATION SECURITY

GAO: DOT Could Improve Resilience to GPS Interference Incidents

In January 2020, DOT began analyzing user reports of potential GPS interference across all transportation modes to identify incidents and support federal investigations. Through this process, DOT identified 196 potential GPS interference incidents from January 2020 through May 2022.

By **Homeland Security Today** December 17, 2022

Share | Facebook | Twitter | Linkedin | Email

GPS can improve transportation safety including aiding emergency response, but is vulnerable to interference from radio signal jamming or other sources. The Department of Transportation (DOT) is responsible for identifying GPS interference incidents and improving the transportation sector's ability to withstand and recover from them.

LATEST ARTICLES

AI AND ADVANCED TECH
TSA Opens it's HQ LIFT Cell/Innovation Lab

AI AND ADVANCED TECH
How Artificial Intelligence Can Reshape Homeland Security in 2024

CBP
Louisville CBP Intercepts Counterfeit Jewelry

BORDER SECURITY
Woman Dies Following Fall From International Border Barrier Near Clint, Texas

CUSTOMS & IMMIGRATION
USCIS Poised to Increase Immigration Filing Fees

Load more >

PTA

Some GPS Receivers Can Be Readily Spoofed

Lloyd's List

Search the site

TAGS: Cyber | Piracy and Security | Containers

EMAIL

War zone GPS jamming sees more ships show up at airports

Surge in ships hit by signal interference in eastern Mediterranean Sea over past few days, while problem is also worsening in the Black Sea

05 Apr 2024 | ANALYSIS

More than 100 cargo-carrying vessels appeared to show up in Beirut airport yesterday. AIS manipulation, common in the region since Hamas' October 7 attack on Israel, has taken off

Subscribe to newsletters

Forbes

FORBES > BUSINESS > AEROSPACE & DEFENSE

FAA Tells Pilots To Go Analogue As GNSS 'Spoofing' Incidents Increase

Feb 3, 2024, 06:21am EST

Marisa Garcia Senior Contributor

I offer an insider's view of the business of flight.

Follow

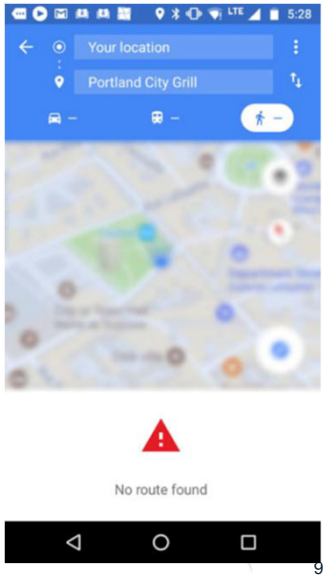
Spoofing Incident Report (Redacted)

An Illustration of Cascading Security Failure

An accidental GNSS spoofing event at ION GNSS+2017 leads to problems with cell phones

Logan Scott
10/3/2017

- Accidental spoofing at ION GNSS+ 2017
  - GPS simulator radiating low power signals deep indoors
  - Some mobile devices reported European location, date of 2014
  - Associated secondary problems with email and text messaging



Satnav Systems Occasionally Have Problems

GPS error caused '12 hours of problems' for companies

4 February 2016

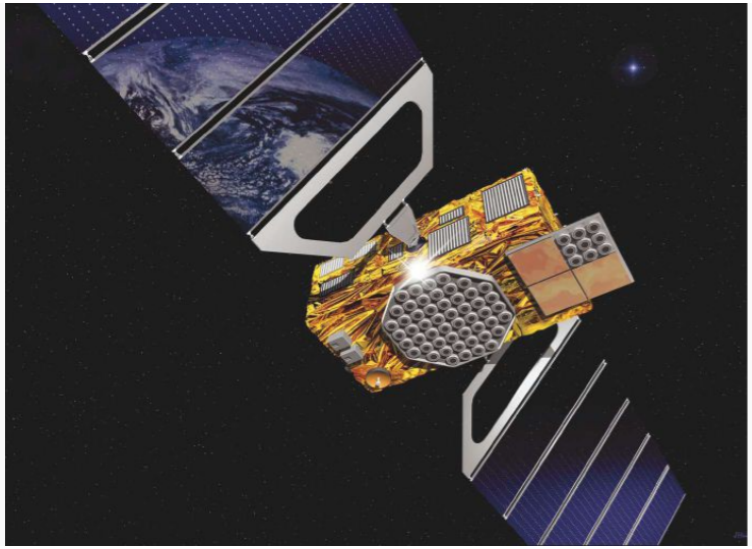
System engineers were "called out of bed" over the problems

By Chris Baraniuk
Technology reporter

Several companies were hit by hours of system warnings after 15 GPS satellites broadcast the wrong time, according to time-monitoring company Chronos.

Lessons to be Learned from Galileo Signal Outage

October 1, 2019 By Inside GNSS



Russia's GLONASS and the Chinese BeiDou system have also experienced technical glitches, of greater or lesser severity. But what happened to Galileo in July 2019 was unprecedented. By the European Commission's own account, the total system failure lasted from 10–17 July. During that time, according to the European GNSS Agency (GSA), "A team composed of GSA experts, industry, ESA and Commission, worked together 24/7 to address the incident."

PTA

PNTAB's Recommendation: GPS Use Needs More…

Protecting

Toughening

Augmenting

Protect, Toughen, and Augment Civil Use of GPS

- Protect: Measures that prevent or remove conditions that degrade, distort, or deny GPS use:
  - Spectrum management that maintains a “clean radio frequency environment” for GPS receivers
  - Education, policies, laws, and enforcement that deter intentional interference and spoofing
  - Capabilities that promptly detect, characterize, and remove unintentional or malicious sources of significant interference or spoofing
  - Steps that ensure the GPS Space and Control Segments meet the GPS Performance Standard even in the presence of challenges (natural events, unintentional events, or malicious actions)
- Toughen: Measures that make GPS use more robust against challenges and threats
  - Satellites that transmit modernized signals that help receivers be robust—more power, more frequencies, resistant to spoofing
  - Control segment that reliably operates modernized signals
  - User devices that robustly and competently employ GPS signals and enhancements*
- Augment: Provision of GPS enhancements* as well as provision and use of alternate Positioning, Navigation, and Timing sources that complement, back up, or replace (partly or entirely) use of GPS

*Enhancements help receivers improve (e.g., accuracy, integrity, robustness) their processing of GPS signals; examples include: differential services such as Satellite-Based Augmentation Systems and Real-Time Kinematic services, the proposed GPS High Accuracy and Robustness Service (HARS), controlled reception pattern antennas, inertial aiding

PTA Framework

		Possible Challenges and Threats to GPS Use					
		Space Weather	Interference/ Jamming of Receivers	Spoofing of Receivers	Error/Failure of Satellites, Monitoring, Control	Attack on Satellites, Monitoring, Control	…
Defenses and Mitigations	Protect						
	Toughen						
	Augment						

- Protect, Toughen, or Augment can address challenges and threats
  - Protecting GPS means less need for Toughening and Augmenting GPS
  - Toughening GPS means less need for Protecting and Augmenting GPS
  - Any technologies used for Augmenting GPS still need to be Protected and Tough
- Users have finite resources—risk management relies on probability of different challenges and threats to GPS use

PTA

Status of Protecting, Toughening, and Augmenting Use of GPS for Critical Infrastructure

- Protecting remains far from complete
  - Still potential for strong adjacent band interference to GNSS receivers
  - Some progress toward a nationwide capability for interference monitoring and removal, but a long way to go
- Export controls hinder the most capable GNSS receiver Toughening—adaptive antijam antenna systems/controlled reception pattern antennas (CRPAs)
- Owners/operators lack needed information for Toughening and Augmenting
  - Users expected to implement risk-informed use of PNT services, but how do users know the risks of GPS failing to provide useful signals due to adversarial or natural events?
  - User investment in Toughen vs. Augment depends on likelihood that GPS provides useful signals in presence of challenges and threats
  - Lacking USG commitment for timely removal of significant interference—what backup is needed?
  - Users lack skills and facilities to evaluate robustness and competence of PNT systems
- Nationally, no evaluation of critical infrastructure progress in Toughen and Augment
  - "You can't improve what you don't measure." *Attributed to Peter Drucker*

PTA

PTA Responsibilities

- Protecting GPS is a Government responsibility
  - FCC regulates spectrum use "for the orderly development and operation of broadcast services" [1]
  - DoC leads "protect the radio frequency spectrum used by GPS and its augmentations through appropriate domestic and international spectrum management and regulatory practices" [2]
  - DoT, DoD, and DHS share "implement Federal and facilitate State, local and commercial capabilities to monitor, identify, locate, and attribute space-based PNT service disruption and manipulations within the United States that adversely affect use of space-based PNT for transportation safety, homeland security, civil, commercial, and scientific purposes" [2]
- Government and users share responsibility for Toughening and Augmenting
  - Critical infrastructure owners and operators expected to have responsible use of PNT services [3]
    - Risk-informed use of PNT services, managing risks from disruption and manipulation of PNT services
  - DoT, DoE, DHS shall each develop plans to engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services [3]
  - OSTP shall coordinate the development of a national plan for the R&D and pilot testing of additional, robust, and secure PNT services that are not dependent on GNSS [3]
    - Plan shall also include approaches to integrate and use multiple PNT services to enhance resilience of critical infrastructure

1. Federal Register :: Agencies - Federal Communications Commission
2. Memorandum on Space Policy Directive 7, gps.gov
3. Executive Order 13095

Today's PTA-Focused Session: Suggest Near-Term Pragmatic Ways to Improve Critical Infrastructure

- "Raise the bar" but accept less than perfection—achieve "herd immunity"
- Use what's available or can be readily available
- Focus on actionable steps that have tangible near-term results
- Provide advice and recommendations to different stakeholders
  - Government
    - Protecting GNSS spectrum use
    - Detecting, characterizing, removing significant sources of interference
    - Toughening receivers for aviation and other safety of life applications
    - Providing information to owners and operators: risks to use of GPS, commitments to interference removal
  - User device manufacturers
    - Specifying, designing, testing, publicizing robustness and competence of user devices
  - Critical infrastructure owners and operators
    - Selecting devices for toughness and competence
    - Adopting augmentations

PTA

Today's PTA Agenda

- 10:30 to 11:30 PTA Overview
- 11:30 to 12:30 Lunch
- 12:30 to 1:45 Protect, with Board Discussion
- 1:45 to 2:00 Break
- 2:00 to 3:15 Toughen, with Board Discussion
- 3:15 to 3:30 Break
- 3:30 to 4:45 Augment, with Board Discussion
- 4:45 to 5:00 PTA Summary
- 5:00 to 6:00 Board Deliberations
- 6:00 Adjourn