Interference Detection and Mitigation (IDM) And GNSS Jammers

United Nations Workshop on the Applications of GNSS
December 06, 2022
Rick Hamilton, U.S. Coast Guard Navigation Center
This presentation does not cover government sponsored jamming and testing
Jammers for Sale

GPS Jammers
To prevent GPS monitoring on your person, cell phone, or vehicle, a GPS signal blocker will stop tracking signals. Maintain your privacy, keep your movements private, and avoid unauthorized surveillance by utilizing a jamming device.

GPS Jammer
For car, truck, bus, van, or even boat security, stop GPS tracking signals by simply plugging this into any cigarette lighter. It will protect you from being located.

GPS Mini
One of the best GPS signal units available for sale, this pocket model will help you defeat GPS tracking. Block tracking signals on your person or vehicle in a 10 meter (30 foot) radius. Give those following your…

Cell and GPS
One of our most popular combinations - silence all nearby mobile phones as always on local signal strength.

High Power Component
Not Rated
If you need a large area of coverage for military or law enforcement applications, then this high power product is for you. This high power unit will cover up to 100 Meters, and is built in an aluminum alloy case that is…

Cell GPS Mini

Compare Selected  Add to Cart
Why Are Jammers Prohibited?

- Jammers do not just weed out noisy or annoying conversations and disable unwanted GNSS tracking.

  Jammers can prevent emergency phone calls from getting through.

  Can interfere with law enforcement communications.

  Jammers can interfere with safety of life services.
Known incidents of Interference

- Jammers' overwhelm anti-theft devices on cars and Trucks. 46 luxury cars returned to Port of Los Angeles discovered with GPS jammers attached to the batteries
- Have been used in vicinity of airports disrupting air traffic
- Establishing quiet zones and text-free zones in Churches and Schools
- Used to defeat the fleet tracking devices in company cars and trucks for theft of high value pharmaceuticals
- Used to defeat attempts to document road use for taxes
- These uses of jammers are illegal!
- Used to disrupt communications during commission of a robbery
- Used in vicinity of a major port disabling GNSS on large cruise ships attempting to dock
Interference at a “Highly Automated Container Port” facility

Estimated throughput: 33.62 million TEUs in 2013

One ship can bring as many as 19,000 20ft containers

TEU = One 20 ft container
Interference Reporting in the U.S.

- U.S. process starts with problem report to NAVCEN or FAA
- Different than ITU form
  - Problem rpt vs After action Rpt
- Service Center triage to confirm problem
- Initial interagency conference call to provide for a coordinated government response
- Priority assigned will determine level of response and agencies involved
- Phone system automatically connects all involved with that level of priority event
Operational impact of disruption determines priority level assigned

• **SEVERE** (Active or Intermittent)
  • Operational Effects: **Severe**
  • GPS anomalies or disruptions affecting one or more user segments or Critical Infrastructure

• **MODERATE** (Active or Intermittent)
  • Operational Effects: **Moderate**

• **LOW** (Active or Intermittent)
  • Operational Effects: **Minimal (or None)**

» E-mail lists provide for situation report distribution to all who sign up for that level of priority event

» Initial Priority level assigned may be upgraded once operational impacts are confirmed.

» Additional interagency conference calls may raise level of priority and determine additional resources/agencies required
U.S. Federal Statutes – Communications Act

47 U.S.C. § 302a(b) Manufacturing, importing, selling, offer for sale, shipment or use of devices which do not comply with regulations are prohibited

“No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section.”
Comprehensive GPS jamming prohibition provisions must be incorporated under four different authorities:

- *National Statutes – Legislation*
- *Telecom Agency Rules*
- *The Criminal Code*
- *International Treaties*
The penalty ($850) could have been a lot worse!

A Melbourne taxi driver was recently convicted and fined $850 by the Magistrates Court for recklessly engaging in conduct that would cause substantial interference to radiocommunications (section 197 of the Radiocommunications Act 1992).

The prosecution was the result of a joint operation between the Australian Communications and Media Authority and the Victorian Taxi Services Commission to combat GPS jammer use within the Melbourne taxi industry. The driver, who pleaded guilty, was detected operating a GPS jammer in the CBD through ACMA surveillance techniques.
Australian Response to The Threat

STEP 1

– Tighten the Communications Laws with regards to GNSS Jammer & Spoofer Ownership and Operation... *done*

STEP 2

– Investigate technologies to DETECT and GEO-LOCATE Jammer & Spoofer operations in GNSS bands... *underway*
Conclusion

• The threat from jammers is real and growing.

• Jammers are being used to commit crimes.

• “Personal Privacy Jammers” are being used to defeat company tracking and road use monitoring.

• To fully utilize all the benefits and efficiencies of GNSS, it is in all our best interests to consider enacting laws to combat the proliferation and use of illegal jammers in our countries.
Back Up Slides

For Reference
“No person shall use or operate any apparatus for the transmission of energy or communications or signals by radio within the United States except under and in accordance with the Communications Act and with a license granted under the provisions of the Communications Act.”
47 U.S.C. § 302a(b) Manufacturing, importing, selling, offer for sale, shipment or use of devices which do not comply with regulations are prohibited

“No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section.”
“No person shall willfully or maliciously interfere with, or cause interference to, any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government.”
Any person who is determined by the Commission, in accordance with paragraph (3) or (4) of this subsection, to have—(A) willfully or repeatedly failed to comply substantially with the terms and conditions of any license, permit, certificate, or other instrument or authorization issued by the Commission; (B) willfully or repeatedly failed to comply with any of the provisions of this chapter or of any rule, regulation, or order issued by the Commission under this chapter or under any treaty, convention, or other agreement to which the United States is a party and which is binding upon the United States; (C) violated any provision of section 317 (c) or 509 (a) of this title; or (D) violated any provision of Section 1304, 1343, 1464, or 2252 of title 18; shall be liable to the United States for a forfeiture penalty. “
“Violation with willful and knowing intent Any electronic, electromagnetic, radio frequency, or similar device, or component thereof, used, sent, carried, manufactured, assembled, possessed, offered for sale, sold, or advertised with willful and knowing intent to violate section 301 or 302a of this title, or rules prescribed by the Commission under such sections, may be seized and forfeited to the United States. “
Regulations in the U.S.

Telecom Agency Rules – FCC

47 C.F.R. § 2.803(a)

- marketing is prohibited unless devices are authorized and comply with requirements…or
- (2) “In the case of a device that is not required to have a grant of equipment authorization issued by the Commission, but which must comply with the specified technical standards prior to use, such device also complies with all applicable administrative (including verification of the equipment or authorization under a Declaration of Conformity, where required), technical, labeling and identification requirements specified in this chapter.”
47 C.F.R. § 2.803(e)(4) – marketing is defined as “sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease.”
The Criminal Code
(Enforced by the Department of Justice)

• Title 18 of the U.S. Code (U.S.C.) contains the criminal and penal code of the U.S. government. It addresses federal crimes, criminal procedures, and general provisions.

• Section 32(a) includes a prohibition on acts that destroy or endanger an aircraft, including:
  • Interference with a navigation facility with intent to endanger the safety of any person or with a reckless disregard for the safety of human life
  • Communication of information known to be false and endangering the safety of any such aircraft in flight.
The Criminal Code

- Title 18, Section 35 - prohibits communication of information known to be false regarding an attempt made to do any act prohibited by 18 U.S.C.

- Title 18, Section 1030 (a)(5) – prohibits damaging a computer system.
The Criminal Code

- Title 18, Section 1362 - prohibits willful or malicious interference to U.S. government communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1362)

- Title 18, Section 1367(a) - prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1367(a))
The Criminal Code

- Section 46308 of 49 U.S.C. stipulates that “a person shall be fined under title 18, imprisoned for not more than 5 years, or both, if the person:

  1. with intent to interfere with air navigation in the United States, exhibits in the United States a light or signal at a place or in a way likely to be mistaken for a true light or signal established under this part or for a true light or signal used at an air navigation facility;

  2. after a warning from the Administrator of the Federal Aviation Administration, continues to maintain a misleading light or signal;

  3. knowingly interferes with the operation of a true light or signal.”
The Criminal Code

- 49 U.S.C. section 46308 and 18 U.S.C. sections 32(a)–35 are referenced within FAA Order 6050.22c [5-3], which contains procedures for investigating and reporting radio frequency interference affecting the NAS.

- FAA Order 6050.22c includes an interagency agreement between the FAA, Federal Bureau of Investigation, and FCC on procedures the three agencies should follow to effectively interact in an attempt to locate, identify, and resolve any deliberate RFI acts such as “phantom controller” incidents.