Interference Detection and Mitigation
and
GNSS Jammers

This presentation does not cover government sponsored jamming and testing

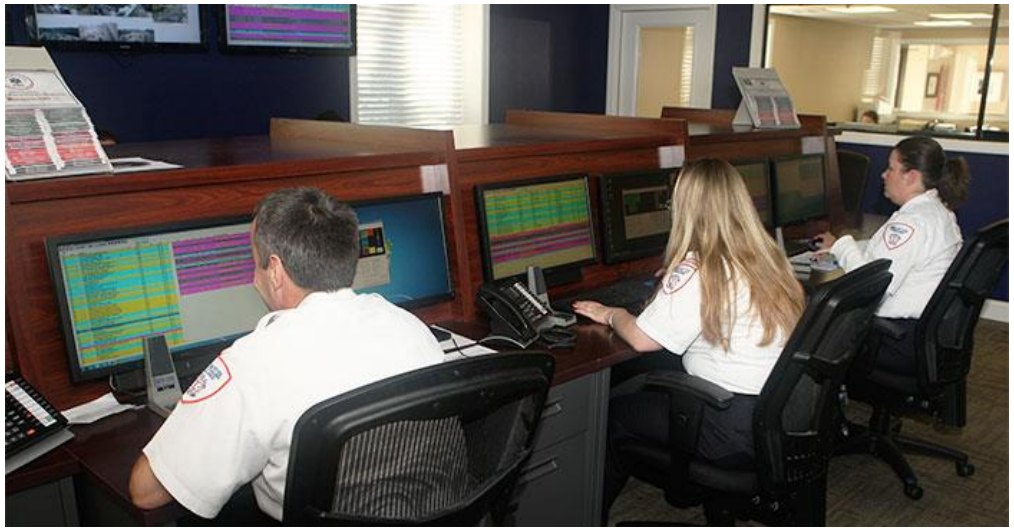
Why Are Jammers Prohibited?

- **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

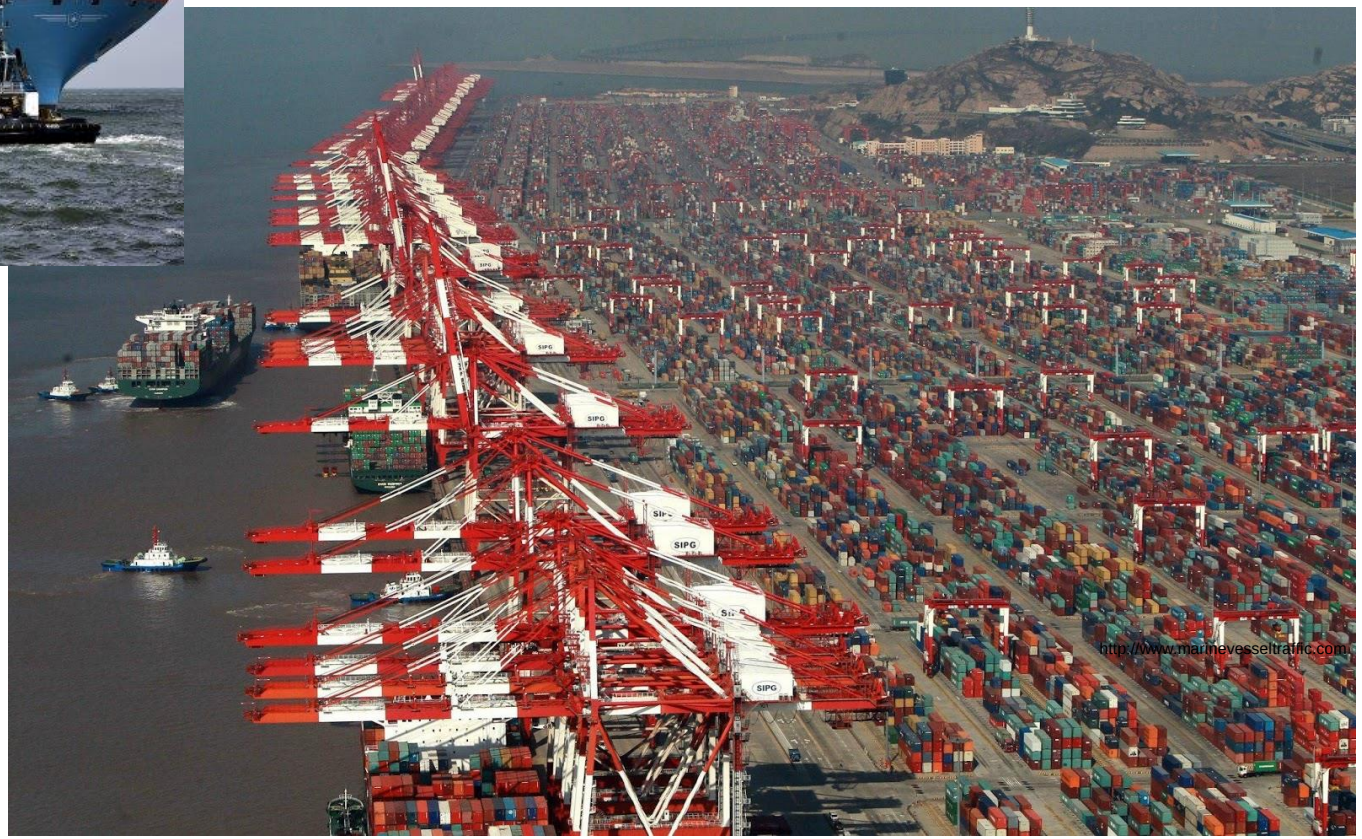
- Used to defeat the fleet tracking devices in company cars and trucks for theft of high value pharmaceuticals
- Used to defeat attempts to document road use for taxes
    - **These uses of jammers were <u>illegal!</u>**

- 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

Reuters

Estimated throughput:
33.62 million TEUs in 2013

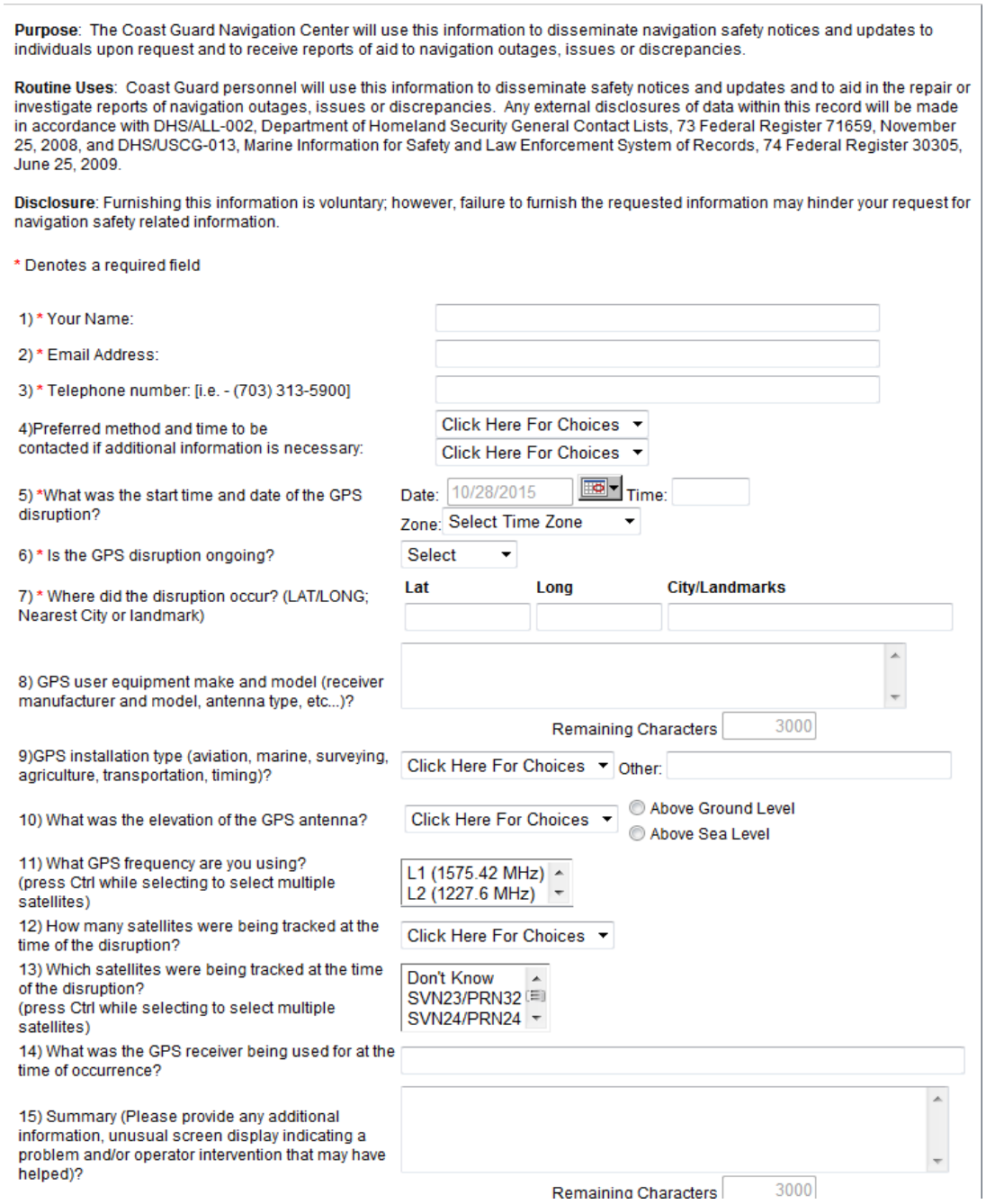


One ship can bring as many as 19,000 20ft containers

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



Purpose: The Coast Guard Navigation Center will use this information to disseminate navigation safety notices and updates to individuals upon request and to receive reports of aid to navigation outages, issues or discrepancies.

Routine Uses: Coast Guard personnel will use this information to disseminate safety notices and updates and to aid in the repair or investigate reports of navigation outages, issues or discrepancies. Any external disclosures of data within this record will be made in accordance with DHS/ALL-002, Department of Homeland Security General Contact Lists, 73 Federal Register 71659, November 25, 2008, and DHS/USCG-013, Marine Information for Safety and Law Enforcement System of Records, 74 Federal Register 30305, June 25, 2009.

Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information may hinder your request for navigation safety related information.

* Denotes a required field

1) * Your Name:

2) * Email Address:

3) * Telephone number: [i.e. - (703) 313-5900]

4)Preferred method and time to be contacted if additional information is necessary: Click Here For Choices / Click Here For Choices

5) *What was the start time and date of the GPS disruption? Date: 10/28/2015 Time: Zone: Select Time Zone

6) * Is the GPS disruption ongoing? Select

7) * Where did the disruption occur? (LAT/LONG; Nearest City or landmark) Lat Long City/Landmarks

8) GPS user equipment make and model (receiver manufacturer and model, antenna type, etc...)? Remaining Characters 3000

9)GPS installation type (aviation, marine, surveying, agriculture, transportation, timing)? Click Here For Choices Other:

10) What was the elevation of the GPS antenna? Click Here For Choices Above Ground Level Above Sea Level

11) What GPS frequency are you using? (press Ctrl while selecting to select multiple satellites) L1 (1575.42 MHz) L2 (1227.6 MHz)

12) How many satellites were being tracked at the time of the disruption? Click Here For Choices

13) Which satellites were being tracked at the time of the disruption? (press Ctrl while selecting to select multiple satellites) Don't Know SVN23/PRN32 SVN24/PRN24

14) What was the GPS receiver being used for at the time of occurrence?

15) Summary (Please provide any additional information, unusual screen display indicating a problem and/or operator intervention that may have helped)? Remaining Characters 3000

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."

Regulations in the U.S.

Comprehensive GPS jamming prohibition provisions must be incorporated under four different authorities:

- *National Statutes – Legislation Communications Act*
- *Telecom Agency Rules – FCC*
- *The Criminal Code – Penalties*
- *International Treaties*

International

- The United Nations Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation is a multilateral treaty that was adopted by the International Conference on Air Law at Montreal on 23 September 1971.

- The Convention signatories agree to prohibit and punish acts that threaten the safety of civil aviation. It entered into force on 26 January 1973 after ratification by 10 nations. As of today, the Convention has 188 signatories.

- Several of the U.S. laws relevant to intentional interference and spoofing of civil aviation GNSS applications were enacted to satisfy obligations made per this Convention.

Spectrum Enforcement Actions

Complaint from a cell provider in Florida that its cell phone tower sites had been experiencing interference:

- Forfeiture Order affirms proposed $48,000 forfeiture against a man for using a cell phone signal jammer in his car while commuting to and from work on a Florida highway over a 16-24 month period.

Anonymous complaint alleging that a company was operating signal jammers to prevent its employees from using phones:

- The company will pay $20,500 in civil penalties for unauthorized use for over 2 years of a signal jamming device purchased and mounted in the company's warehouse to prevent employees from using the cell phones while working.

Spectrum Enforcement Actions

- Forfeiture Order proposing a $34,912,500 forfeiture against manufacturing company for marketing 285 models of signal jamming devices
- A retail business sold a cell phone signal blocker device to a private citizen for use in a child care center.
- Omnibus Citation and Order to 20 Online Vendors for marketing signal jamming devices to consumers via the Internet in the United States or its territories.

Canada

Spectrum Management and Telecommunications

Jamming Devices are Prohibited in Canada:That's The Law

July 2011

The importation, manufacturing, distribution, offering for sale, sale, possession and use of radiocommunication jamming devices in Canada are prohibited under sections 4, 9 and 10 of the *Radiocommunication Act*.

What is a radiocommunication jamming device?

A radiocommunication jamming device, also known as a signal silencer, blocker or disabler, is a radiocommunication transmitter designed to interfere with, disrupt, or block radiocommunication signals and services. Although most jamming devices are manufactured for the purpose of disrupting the functioning of wireless cellular networks and low-power communication devices (cordless telephones and cameras, Wi-Fi networks and reception of GPS signals), they can also prevent communication to emergency services (9-1-1, ambulance, fire, police, aeronautical service, etc.).

Over the past few years, Industry Canada has encountered several cases of illegal importation, possession and use of radiocommunication jamming devices.

Legislation

A conviction under the *Radiocommunication Act* carries a fine of up to $5,000 and/or imprisonment not exceeding one year (individual) or a fine of up to $25,000 (corporation), as well as forfeiture of the radio apparatus and possibly an injunction to refrain from activity related to the offence.

For further information on the associated Canadian regulations, please consult: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01329.html.

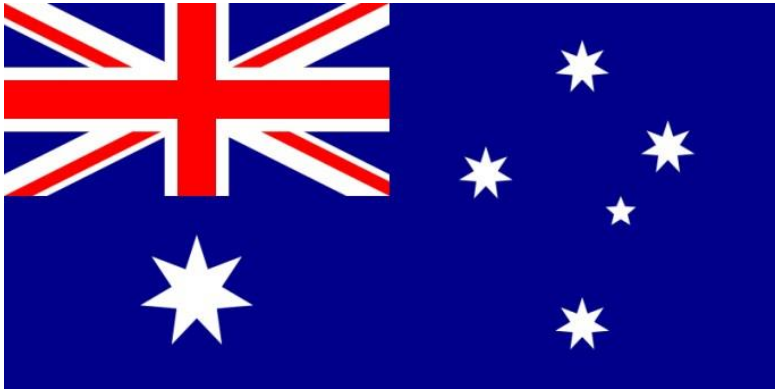
Importation of Equipment

In Canada, radio apparatus, interference-causing equipment and terminal equipment are subject to Canadian regulations. Canadian consumers and others seeking to import radio transmitting equipment into Canada should verify that the equipment meets Industry Canada's technical regulations prior to making any purchases. Jamming devices may be detained or seized at the border, and the importer may, on prosecution, be liable to a fine or to imprisonment.

Penalties

- Administrative Monetary Penalties
  - Civil penalties
  - Up to $10 million ($15 million for subsequent violation) for companies, $25,000 ($50,000 for subsequent violations) for individuals
- Regulatory Offence
  - $5,000 fine and/or one year in prison for individual
  - $25,000 fine for companies

Australia



Australian Offences and Penalties

- Operation or supply of a prohibited device, 2 years' imprisonment or $165,000 fine.
- Causing interference likely to prejudice the safe operation of vessels, aircraft or space object, 5 years' imprisonment or $550,000 fine.
- Causing interference in relation to certain radiocommunications (including rescue and emergency call service police, fire, ambulance, etc), 5 years' imprisonment or $550,000.
- Causing interference likely to endanger safety of another person or cause another person to suffer or incur substantial loss or damage, which attracts a penalty of 5 years' imprisonment or $550,000 fine.
- Reckless conduct which causes substantial interference with radiocommunications, or substantial disruption or disturbance of radiocommunications, which attracts a penalty of 1 year imprisonment.

itnev
FOR AUSTRALIAN B

News | Te

Galleries | Research | Blogs

Home / News / Tech

Taxi driver convicted

Melbourne

By Ry Crozier on .
Filed under Hardw

Like 30 Tweet

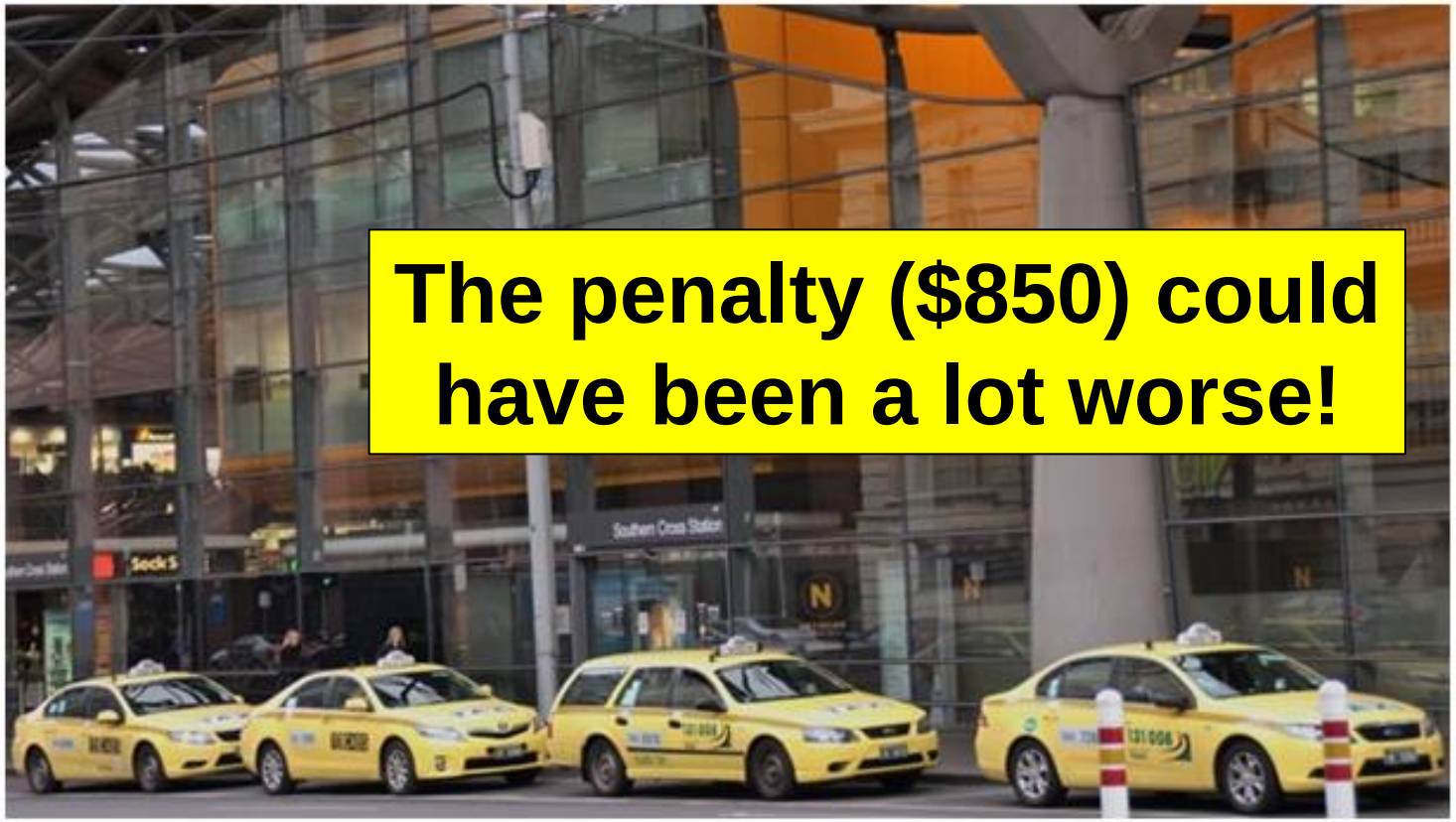
An ACMA inspector monitors a Melbourne taxi rank. (Photo credit: ACMA)

Tags

melbourne, taxi, driver, fine, gps, jammer, illegal

Related Articles

- Equinix commits US$60m to Melbourne data centre
- Melbourne tries again for



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

U.S. Federal Statutes – Communications Act

47 U.S.C. § 301 Unlicensed (unauthorized) operation prohibited.

"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."

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."

U.S. Federal Statutes – Communications Act

47 U.S.C. § 333 – Interference to authorized communications prohibited

– "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."

U.S. Federal Statutes – Communications Act

47 U.S.C. § 503: Forfeitures

"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. "

U.S. Federal Statutes – Communications Act

47 U.S.C. § 510: Forfeiture of communications devices

"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.”

Telecom Agency Rules – FCC

47 C.F.R. § 2.803(e)

- 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.