GNSS Interference Detection and Mitigation

COPUOS Scientific and Technical Subcommittee Meeting

07 February 2017

5 elements

- Spectrum Management in the U.S.
- Status of IDM research in the U.S.
- Spectrum Enforcement Actions
- IDM Reporting
- IDM activities through the ICG

The Problem

- A jammer can *block all radio communications* on any device that operates on radio frequencies within its range.
- Generally *does not discriminate* between desirable and undesirable communications.
- Jammers can:
  - prevent your cell phone from making or receiving calls, text messages, and emails;
  - prevent your Wi-Fi enabled device from connecting to the Internet;
  - prevent your GPS unit from receiving correct positioning signals; and
  - prevent a first responder from locating you in an emergency.

Reported Incidents of Interference

- Jammers overwhelm anti-theft devices on cars and trucks enabling undetected movement
- Have been used in vicinity of airports disrupting air traffic
- Illegally establishing quiet zones and text-free zones in Churches and Schools

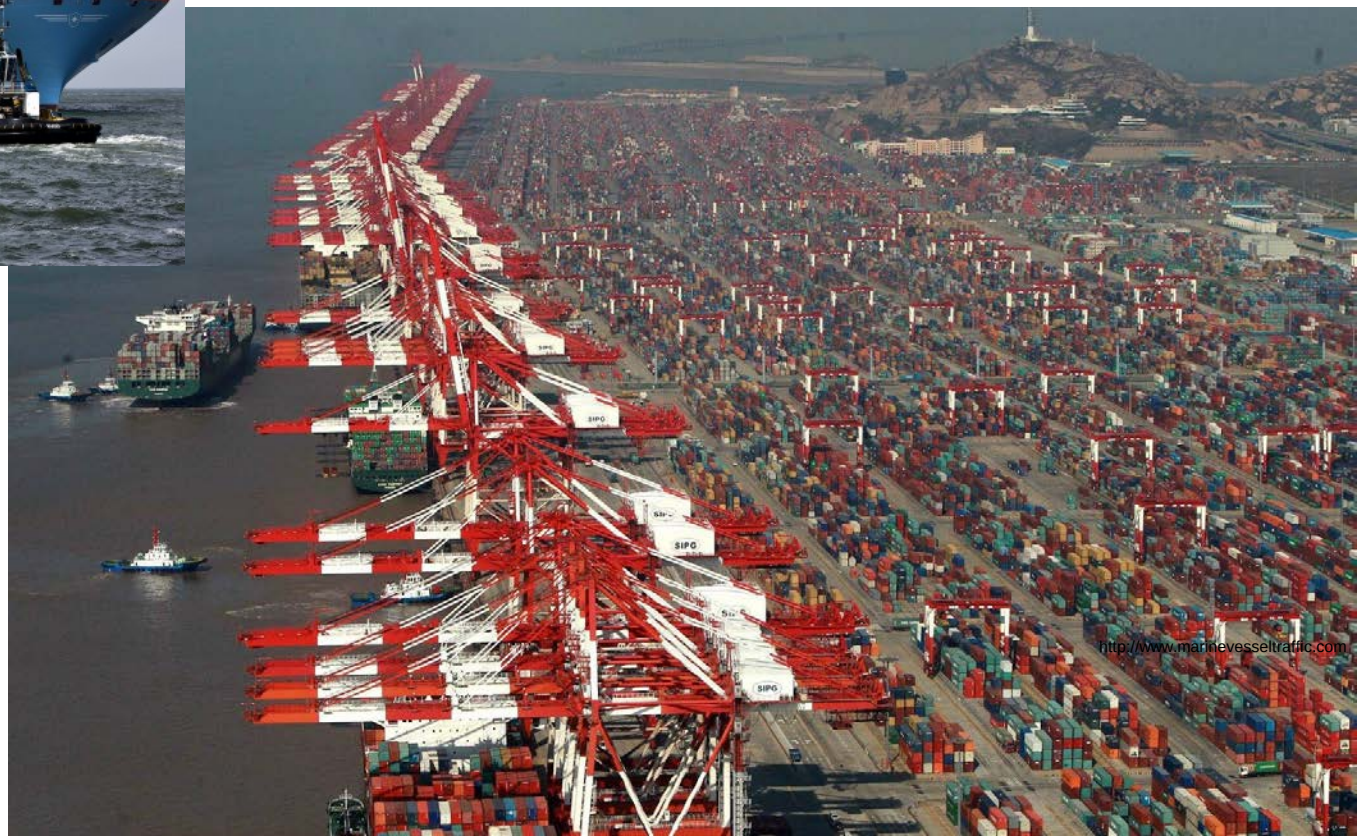
- Facilitating criminal activity
- Used to defeat attempts to document road use for taxes

- Used to defeat the fleet tracking devices in company cars and trucks
- Interfering with port operations
- **These uses of jammers are <u>all illegal in the U.S.</u>**

Interference at a Highly Automated Container Port facility

Reuters

Port of Shanghai throughput: 33.62 million TEUs in 2013



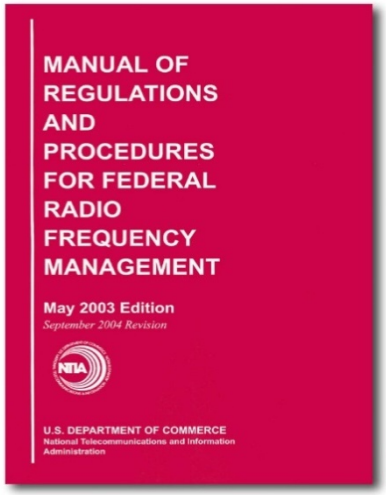
One ship can bring as many as 19,000 20ft containers

TEU = One 20 ft container

U.S. National Spectrum Agencies

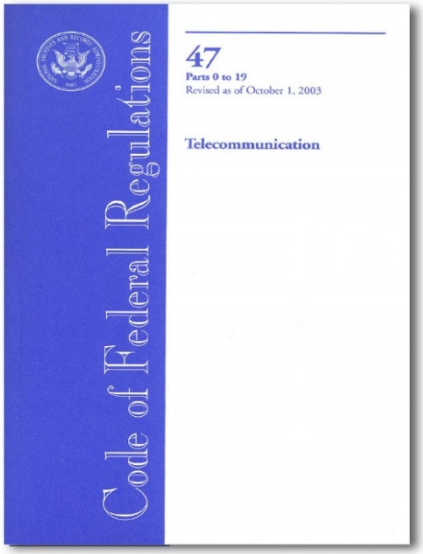
- In the U.S. there are three categories of allocations
  - Government (Federal)
  - Non-government (includes state and local)
  - Shared
- Spectrum is usually separated and is managed by different agencies:
  - Government (Federal) spectrum: National Telecommunications and Information Administration (NTIA)
  - Non-Government (includes state and local) allocations Federal Communications Commission (FCC)
  - NTIA and and FCC coordinate actions for those bands that are “shared”

International and National Allocations



- In general, national frequency allocations are aligned with the ITU table of frequency allocation

- However, though they are not identical since each nation has sovereign rights to manage its own spectrum, the U.S. pursues harmonized use of the radio frequency spectrum".



Recent policies that impact IDM R&D

Implementation Roadmap for National Critical Infrastructure and Resilience Research and Development Plan – released by the White House on 12/20/16

- Enhancing the next generation of civil GPS signals and improving interference detection and mitigation (IDM) approaches for PNT services can increase the robustness and resilience of PNT systems and services.
- Activities for IDM can support R&D efforts to establish a nationwide ability to identify, detect, locate, auto-report, and mitigate GPS disruptions (e.g., interference, jamming, and spoofing). These improvements would enhance the ability of users to share information with stakeholders and enable enforcement actions when appropriate.

Critical Infrastructure Resilience

- Technology enabled by GPS is increasingly yielding benefits
- Need to anticipate, accommodate, and accelerate innovation
- Need to understand and mitigate the risks associated with new technologies
- GPS is now widely used by civil infrastructure users
- With strong support of government we have the responsibility to work with the private, public and international partners to help them become increasingly resilient

Best Practices

In the past 2 years the U.S. has released 2 best practices for mitigating the effects of a localized GPS disruption.

- Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations 6 January 2015
- Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure
- Find these documents at: **www.GPS.gov**
  Look for: Guidance for Critical Infrastructures

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.

U.S. Federal Statutes – Communications Act

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

§ 301 - Prohibits the use or operation of “any apparatus for the transmission of energy or communications or signals by radio” within the United States and its territories unless such use is licensed or authorized.

§ 333 - “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.”

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.

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."

Federal Communications Commission (FCC) Rules

- Section 2.803 - prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 C.F.R. § 2.803)
- Section 2.807 - provides for certain limited exceptions, such as the sale to U.S. government users (47 C.F.R. § 2.807)

The Criminal Code
(Enforced by the Department of Justice)

- 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))

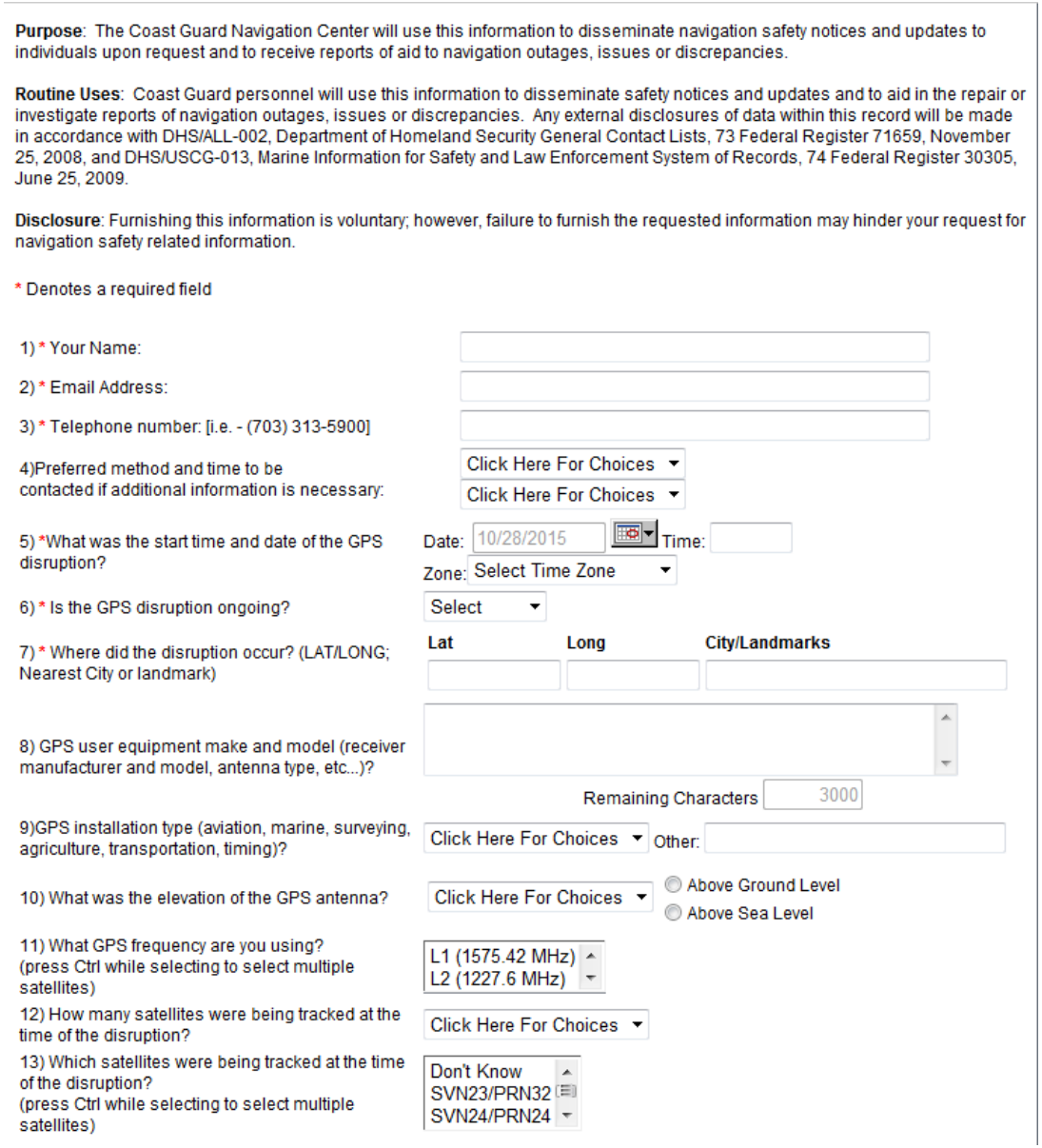
Comprehensive GNSS jamming prohibition provisions must be incorporated under four different authorities:

- *National Statutes – Legislation*
- *Telecom Agency Rules*
- *The Criminal Code*
- *International Treaties*

Interference Reporting

U.S. process starts with problem report to NAVCEN, FCC 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/Discussion on way fwd
- Priority assigned will determine level of response and agencies involved



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

Interference Report Form:
https://www.navcen.uscg.gov/?pageName=gpsUserInput

IDM and the ICG

- At the inception of the ICG, the Working Group on Compatibility and Interoperability was tasked to develop a strategy supporting mechanisms to detect and mitigate sources of electromagnetic interference, taking features of GNSS signals and existing regulatory mechanisms into consideration
- An IDM Task Force was formed by the working group to undertake this work
- Under the newly structured ICG Working Group on Systems, Signals and Services, IDM efforts have been combined with Compatibility and Spectrum Protection under a Sub-group chaired by Japan and the EU
- 5 IDM workshops and 2 IDM& Spectrum seminars have been conducted to date

Interference Detection & Mitigation Task Force

- **Co-Chairs**:
  - **Rick Hamilton, U.S., Co-lead stephen.r.hamilton@uscg.mil**
  - **Weimin Zhen, China, Co-lead crirp_zwm@163.com**

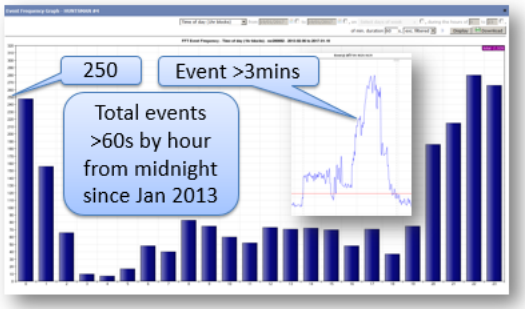
- Members:
  - Attila Matas, ITU attila.matas@itu.int
  - Matteo Paonni, EU matteo.paonni@jrc.ec.europa.eu
  - Stanislav Kizima, Russia kizima@vemail.ru
  - Sergey Mitchenkov, Russia mitchenkov@mail.ru
  - Ivan Malay, Russia malay@vniiftri.ru
  - Igor Zheltonogov, Russia Zheltonogov@geyser-telecom.ru
  - TANG Jing, China blazingtangjing@163.com
  - WEN Xiong, China crirp_xw@163.com
  - SHEN Jiemin, China shenjiemn@bsnc.com.cn
  - Koji Nakaitani, Japan koji.nakaitani.m7u@cao.go.jp
  - Takahiro Mitome, Japan takahiro.mitome.xp@hitachi.com
  - Yoshimi Ohshima, Japan y-ohshima@cb.jp.nec.com
  - Hiroaki Maeda, Japan Hiroaki.Maeda@LighthouseTC.jp
  - Frank Clark, USA

Cooperation and Information Sharing Between Provider Service Centers

Name	Country	URL
Information Analysis Center	Russia	http://glonass-iac.ru/en/
US Coast Guard Navigation Center	U.S.	http://www.navcen.uscg.gov/
William J. Hughes Technical Center WAAS Test Team	U.S.	http://www.nstb.tc.faa.gov/index.htm
European GNSS Service Centre	EU	http://www.gsc-europa.eu/
iGMAS Service Center	China	http://www.csno_tarc.com
QZ-vision	Japan	http://qz-vision.jaxa.jp/USE/en/index
	India	
IGS portal	IGS	http://igs.org/

Significant IDM Technologies

UK Research into GPS Jamming



Handheld Detection

JammerCam™ testing in the UK

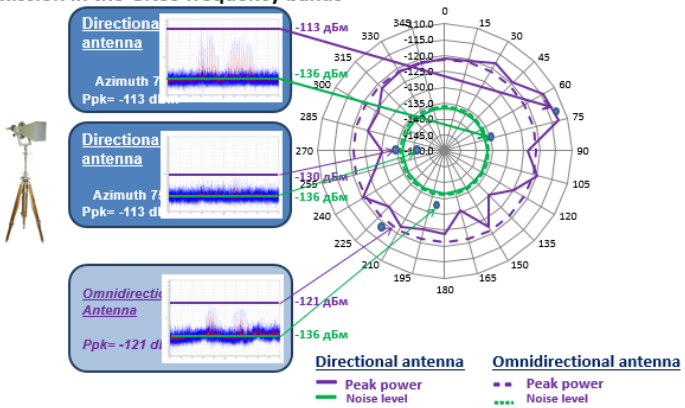
Chronos Technology Research Projects with Innovate UK
GAARDIAN – 2008 - Technology to detect Jamming
SENTINEL – 2011 - Technology to geolocate Jamming
AJR – 2013 – Technology to photograph vehicle with Jammer

Chronos GPS jamming detection technology used in the **Harris Signal Sentry™ 1000** System for geolocation

Recommendations for estimation of electromagnetic environment and Interference environment in GNSS frequency Bands. Content suggestions

***Section 8.* Total estimation of electromagnetic and interference environment**

The basis of the methodological approach - the construction and analysis of special diagrams of the spatial distribution of energy emission in the GNSS frequency bands

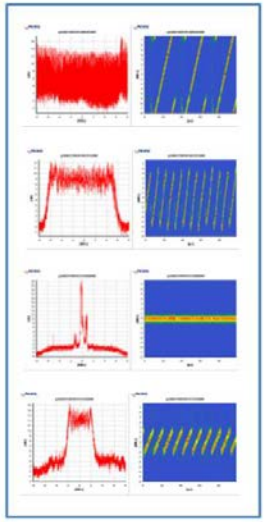


DETECTOR Characterisation

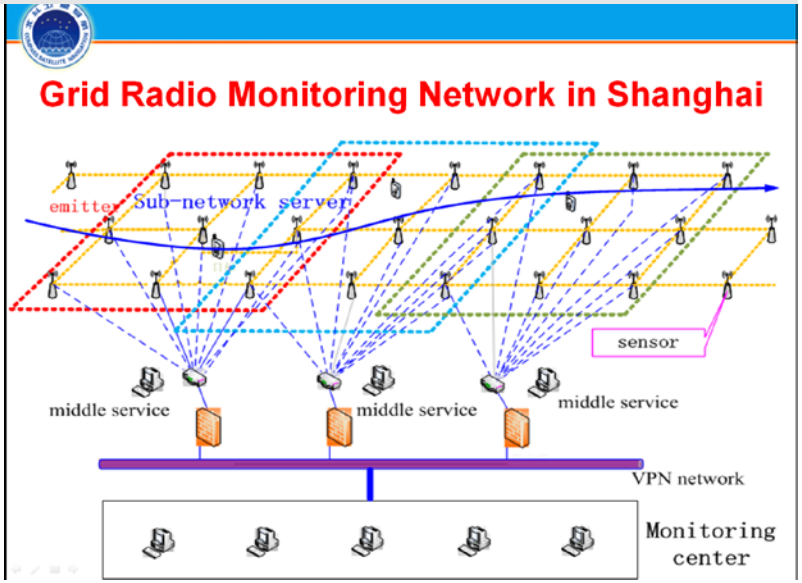
Characterisation and parameterisation of incoming signals

1. Determine likely **impact** on users
2. Differentiate **unintentional** interference from **jamming**
3. **Differentiate** between jammer types
4. Identify **multiple detections** of the same interference versus one-offs
5. Identify **trends** in the evolving threat
6. Develop **countermeasures**
7. **Catalogue** the threats

DETECTOR captures and characterises the threat



Grid Radio Monitoring Network in Shanghai



Crowd Sourcing

Every cell phone can be a GPS jamming detector.
Requires a Public/Private Partnership.

GNSS Spectrum Protection

- Starts with good foundations, the ITU; but it is crucial to protect GNSS spectrum at BOTH international and national levels.
- Compatibility analysis of new radio systems is essential before introducing them into operation to avoid interfering with existing GNSS signals

Interference Detection

- The ITU provides the regulatory framework (Radio Regulations), but it is national regulators that play the key role in finding interferers to GNSS

- Robust enforcement of national and international regulations is vital to limit impacts to GNSS

GNSS Jammers – National Legal Status (As Reported at ICG-9)

Jammers	US	RU	China	EU
manufacture	illegal	illegal	illegal	Nation-by-nation
sell	illegal	illegal	illegal	illegal
export	illegal	illegal	illegal	Nation-by-nation
purchase	Undefined (consumer import illegal)	illegal	illegal	illegal
own	legal	Undefined	Undefined	legal
use	illegal	illegal	illegal	illegal

Your Role

- We encourage you to go back to your national regulators and find out how they are protecting GNSS from interferers.
- Do they realize the vulnerability of GNSS reception?
- Do they appreciate the economic impact of GNSS loss?
- Are they doing enough to protect GNSS spectrum from interference?

FINI

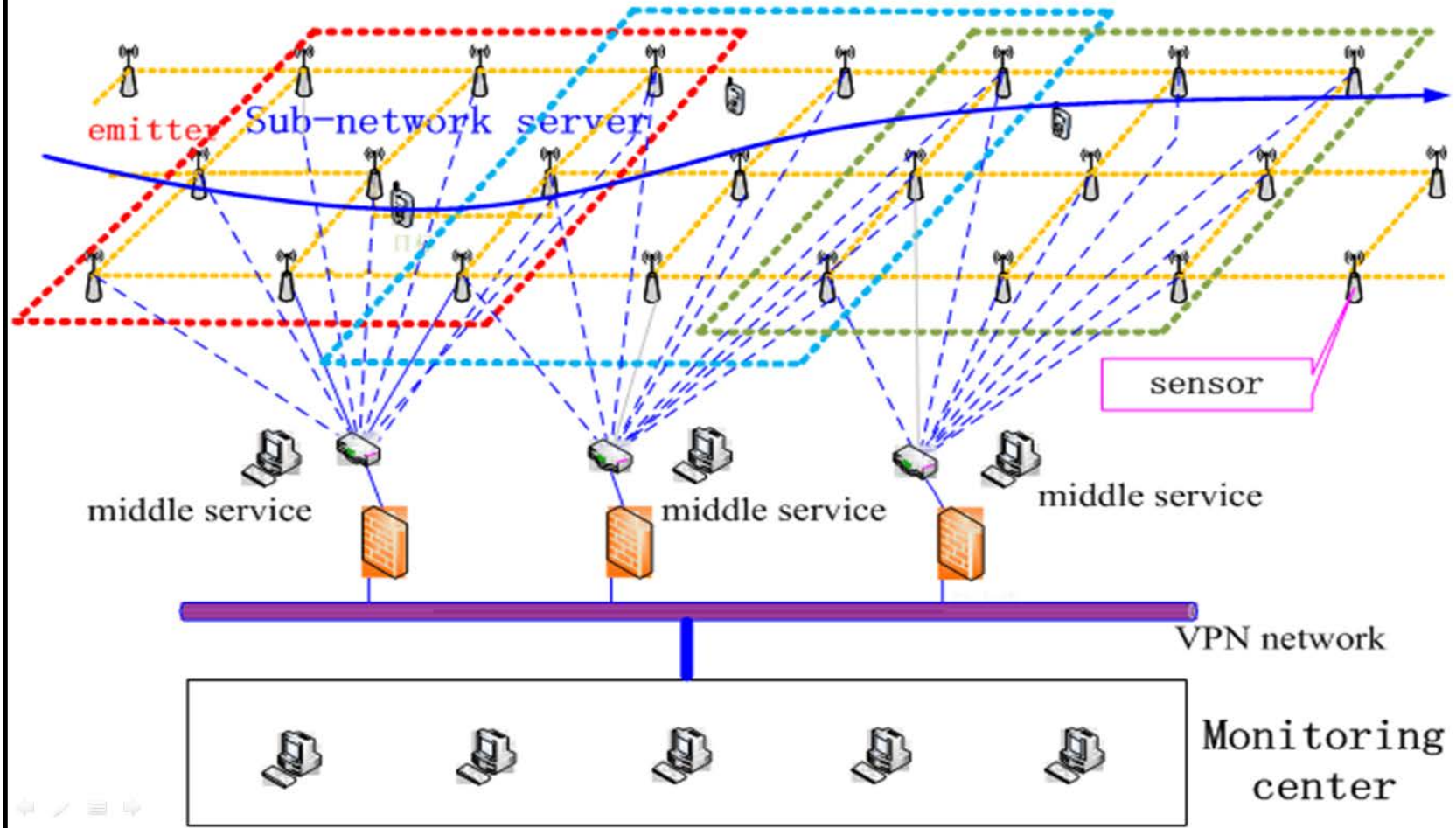
Back up slides

Demonstrated GNSS IDM technologies

China Experimental Grid Radio

Monitoring Network

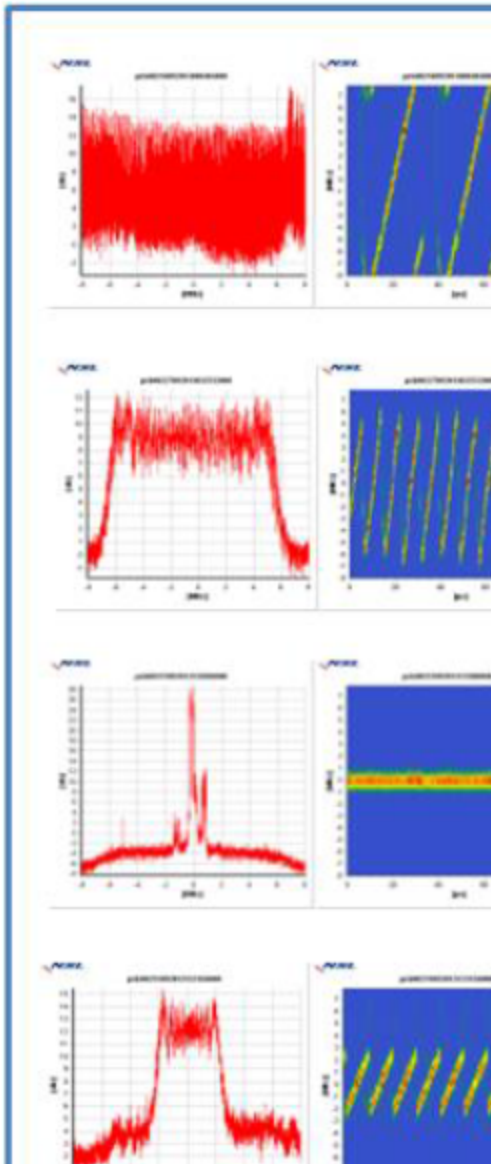
Grid Radio Monitoring Network in Shanghai



DETECTOR Characterisation

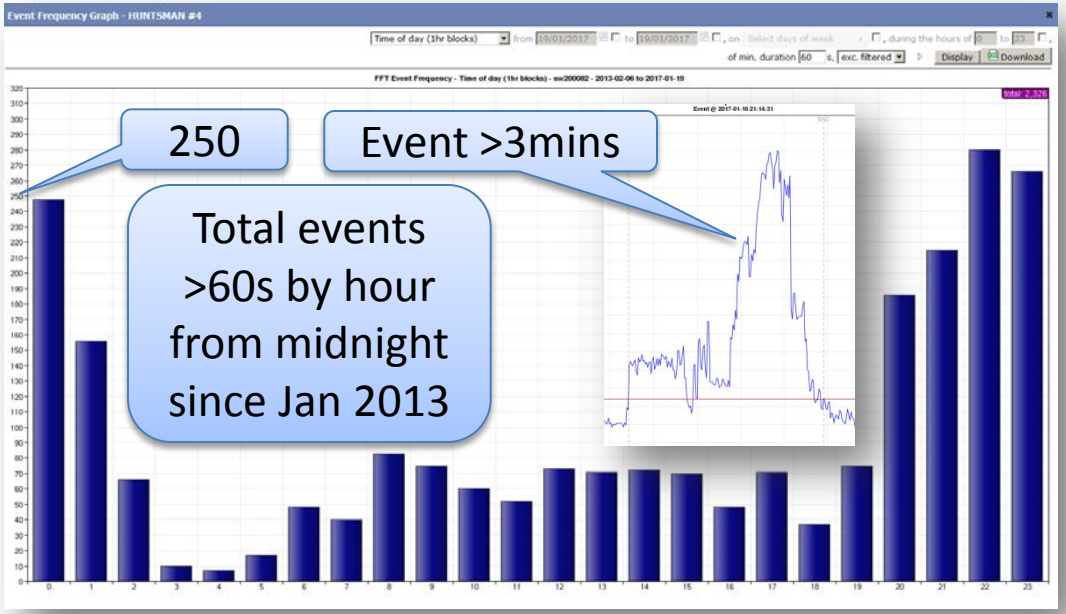
Characterisation and parameterisation of incoming signals

1. Determine likely **impact** on users
2. Differentiate **unintentional** interference from **jamming**
3. **Differentiate** between jammer types
4. Identify **multiple detections** of the same interference versus one-offs
5. Identify **trends** in the evolving threat
6. Develop **countermeasures**
7. **Catalogue** the threats



DETECTOR captures and characterises the threat

UK Research into GPS Jamming



Handheld Detection

JammerCam™ testing in the UK

Chronos Technology Research Projects with Innovate UK

GAARDIAN – 2008 - Technology to detect Jamming

SENTINEL – 2011 - Technology to geolocate Jamming

AJR – 2013 – Technology to photograph vehicle with Jammer

Chronos GPS jamming detection technology used in the **Harris Signal Sentry™ 1000** System for geolocation

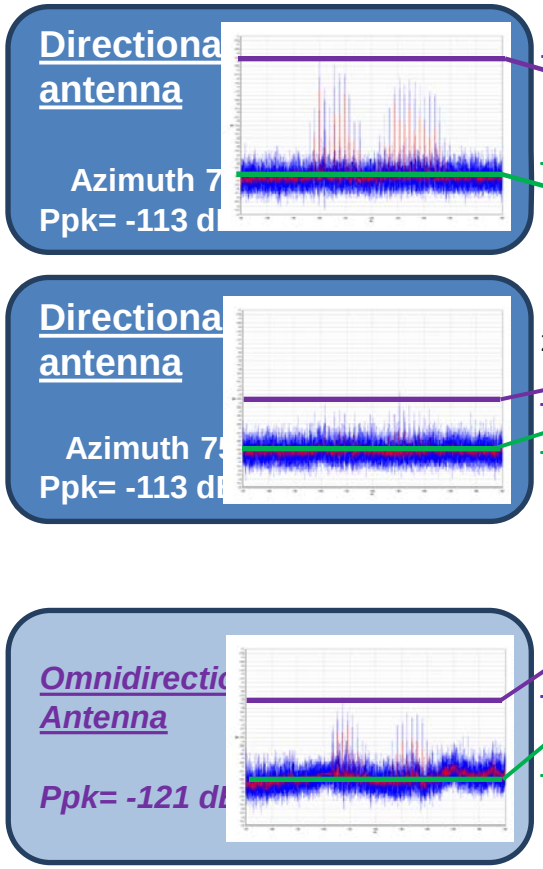
Signal Sentry® 1000 Overview

- Detects and locates sources of GPS signal interference
- Provides location of interference
- Presented in the form of geographical pin mapping
- Provides actionable intelligence to the user
- Leverages Exelis signal domain knowledge of GNSS
- Patented Exelis Technology
- Signal Sentry 1000 data aids Intelligence Led Policing

Assures safety, efficiency, and revenue

Section 8. Total estimation of electromagnetic and interference environment

The basis of the methodological approach - the construction and analysis of special diagrams of the spatial distribution of energy emission in the GNSS frequency bands

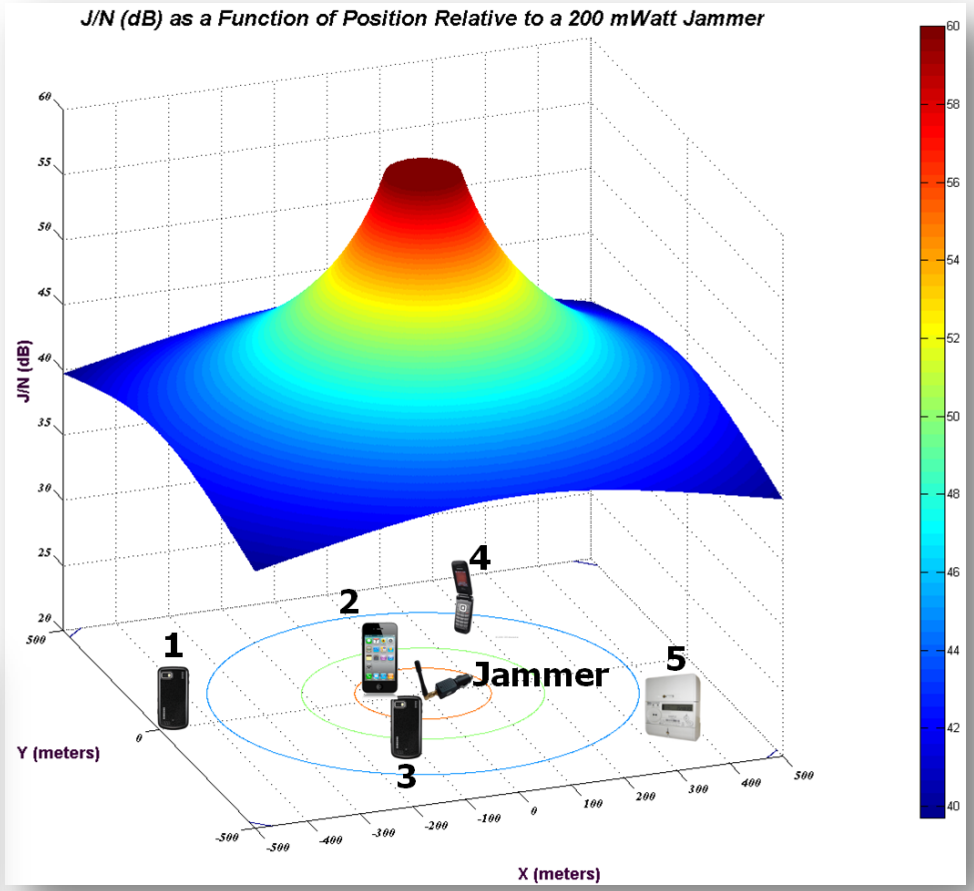


Crowdsourcing for Jammer Detection & Location (J911)

Geographic Coverage Is the Challenge for IDM Systems; Detectable Range May Only Be a Few Hundred Feet and Multipath Effects Can Be Severe

Collaborative Defense

- **Devices Report Jamming Parameters & Own Position to J911**
- **Using Aggregate of Reports, J911 Can Determine Jammer *Position to ~ 40 meters in near real-time***
  - **J911 Can Report Interference Events to Networked Users (Like Traffic Reports)**



from Logan Scott: J911: *The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches*, ION-GNSS-2011, September 20-23, 2011

© Logan Scott / LS Consulting