GOT COMMS?

Recognizing and Mitigating Intentional and Unintentional Interference

Homeland Security

Science and Technology

What is Interference?

Any signal that seriously degrades, obstructs or repeatedly interrupts radio frequency signals

Unintentional Sources

- Spurious emissions, intermodulation, harmonics
- Co-channel or adjacent channel users
- Signal boosters (BDAs)
- Natural phenomena (sun flares)

Intentional Sources

- Illegal jammers
- Unauthorized transmissions

Examples of Interference Sources

Interference Symptoms

Disruption or failure of wireless communications or mapping equipment – including cellular, LMR or GPS systems – for unknown reasons could indicated interference

You may be experiencing spectrum interference if you:

- Can't communicate in areas where you typically have good radio or cell coverage
- Can't communicate with normally reliable base radios or repeaters
- Can't communicate on multiple communications devices using multiple bands
- Notice a significant loss of lock or general failure of GPS systems
- Can significantly improve communications capability by moving a short distance away from a fixed "dead zone"

RECOGNIZING INTERFERENCE

How do you Recognize Interference?

For public safety network technicians, Communications Unit Leaders (COMLs) or anyone in IT, there are 3 basic recommendations

1. **Track reports of equipment malfunctions** – If all operational assets have issues at the same time or if there are repeated issues at the same location, investigate.
2. **Characterize the interference using a spectrum analyzer** – Is there a high noise floor? Is there blocking? What is the BER? Is audio disabled or degraded? Is the pattern variable?
3. **Collect data and report it to the FCC Enforcement Bureau** – Save recordings, spectrum analyzer screen shots and all incident logs (with location tagging), and share with FCC.

Unintentional: Spurious Emissions

What is it?

Any RF signal that isn't deliberately created or transmitted, or signals emitted outside a transmitter's assigned channel and necessary bandwidth (also known as a spur)

Sources

- Non-linear characteristics in transmitters
- Physical placement of components
- Unwanted coupling

Unintentional: Intermodulation

What is it?

Paired spurs on either side of two or more signals appearing in a nonlinear circuit

Sources

- Transmitter-produced intermods
- Receiver-produced intermods
- "Other" radiated intermods

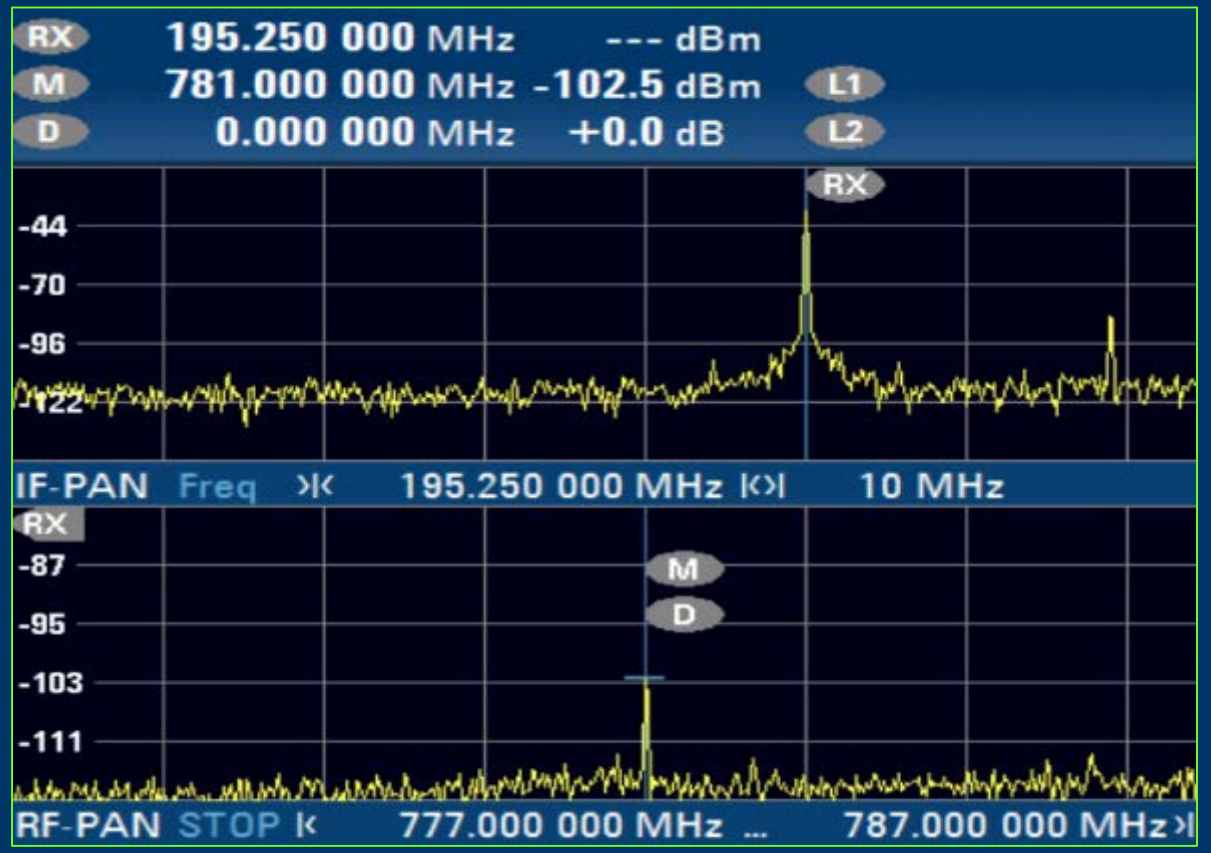
Unintentional: Harmonics

What is it?

Duplicate copy of a signal appearing at some X multiple of the fundamental frequency (e.g., original signal is 50 Hz, harmonics appear at 100 Hz, 150 Hz…)

Sources

- Non-linear characteristics in transmitters
- Misadjusted, poorly maintained or defective communications transmitters



Unintentional: Co-Channel

What is it?

Crosstalk with two different radio transmitters using the same frequency

Sources

- Poor frequency planning and coordination, particularly with multi-agency incidents
- Adverse weather conditions
- Non-UL electronics

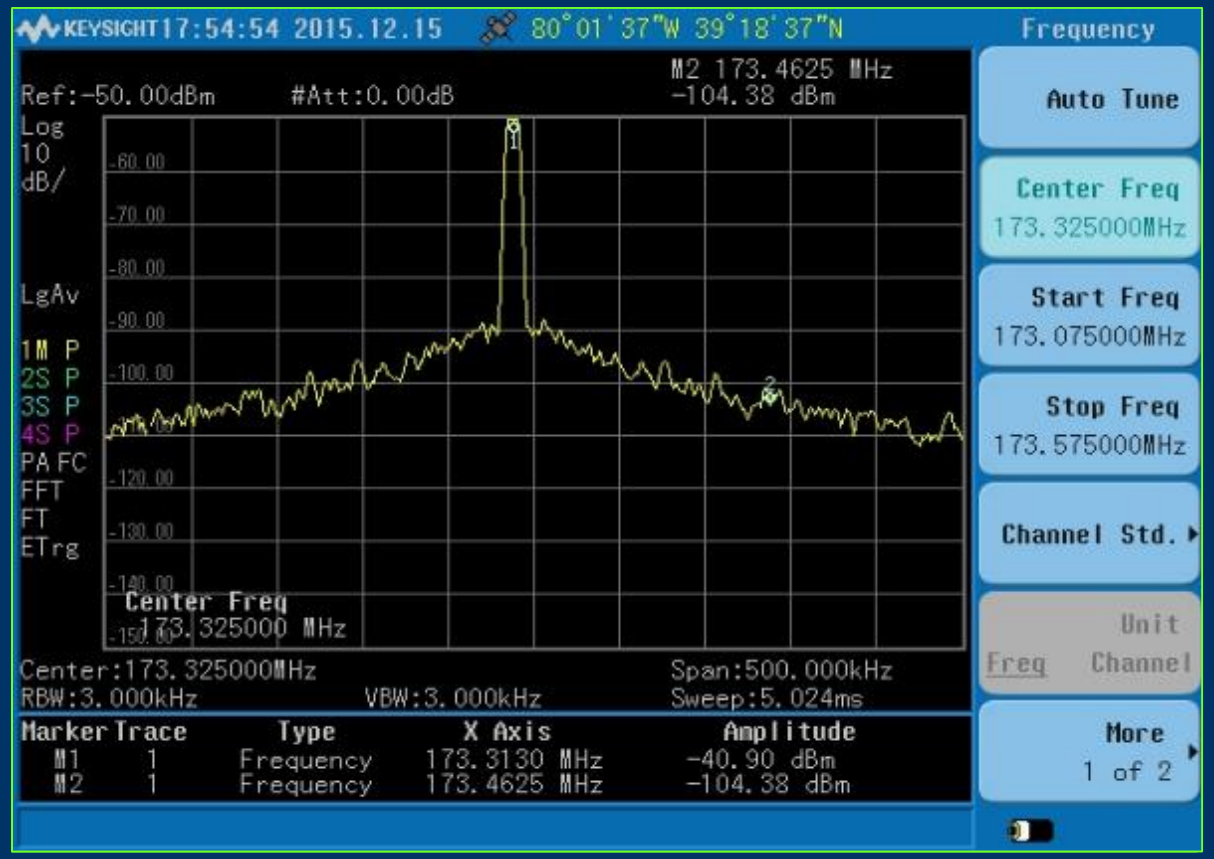
Unintentional: Adjacent-Channel

What is it?

Spurs caused by extraneous power from a signal in an adjacent channel

Sources

- Inaccurate tuning
- Inadequate filtering
- Poor frequency control mechanisms



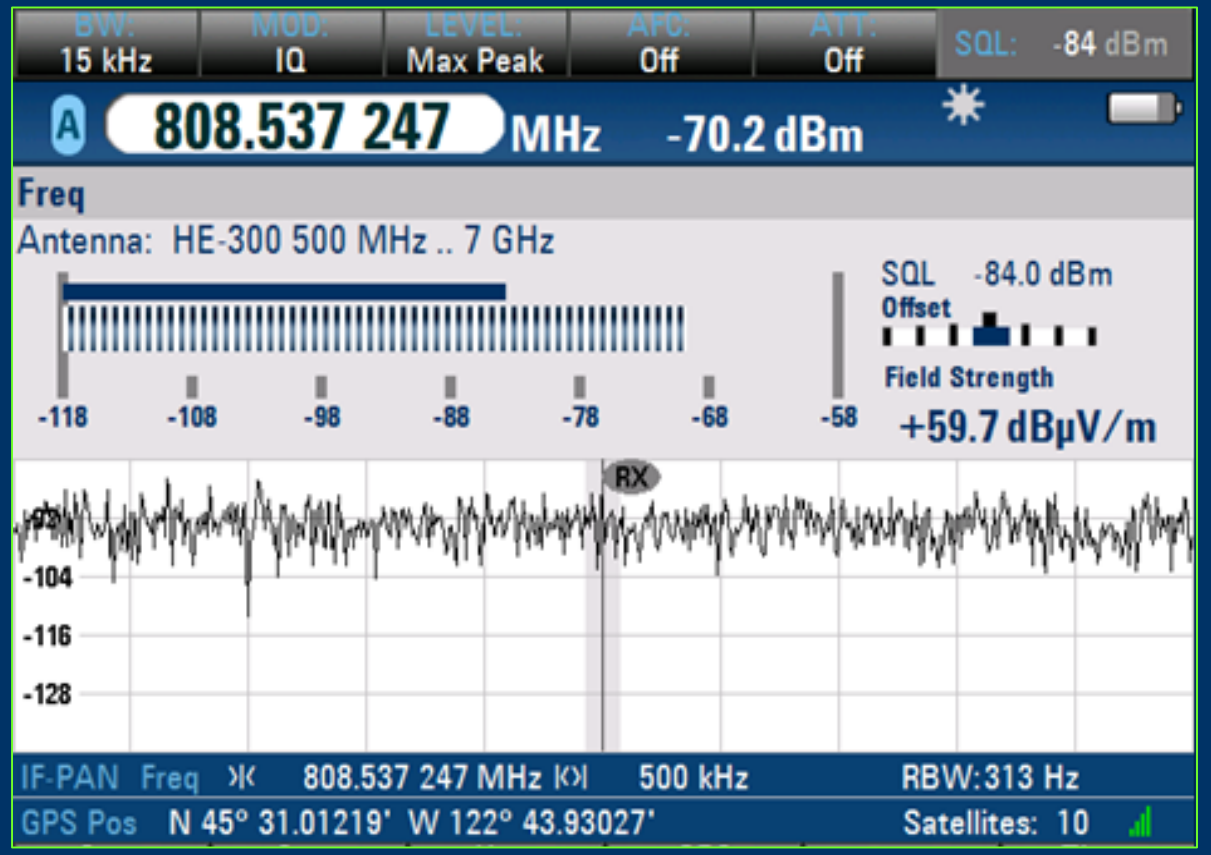
Unintentional: Signal Boosters

What is it?

Malfunctioning and improperly designed or installed signal boosters can cause out of band spurs

Sources

- Defective signal boosters, such as Bi-Directional Amplifiers (BDA), are sometimes accidentally left in buildings and may go rogue, emitting out of band spurs



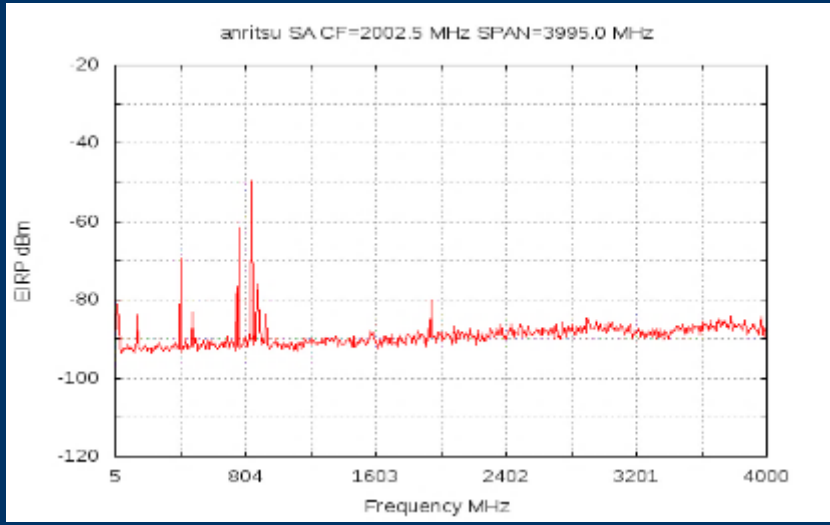
Intentional Interference: Illegal Jammers

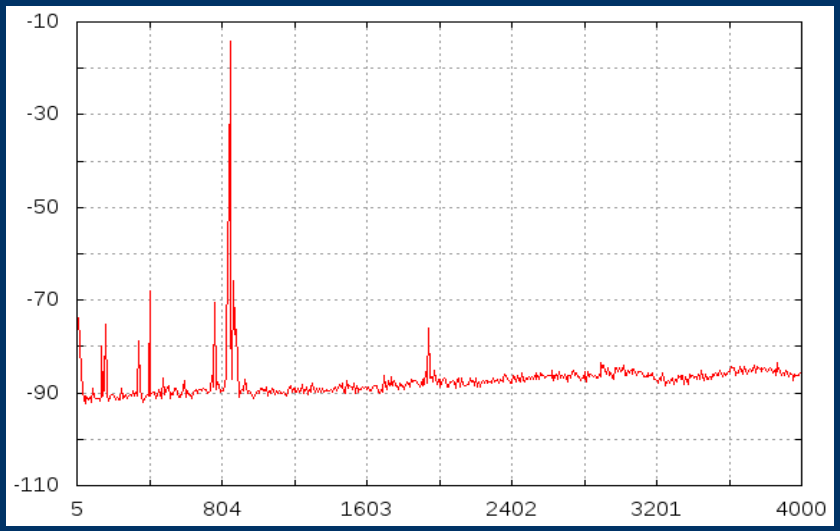
- Jamming devices are designed to emit RF noise over specific bands to overpower signals at the receiver, blocking the intended signal from getting through
- Jammers are often cheaply manufactured overseas and are low-quality electronics, which means that they often emit RF noise outside the intended bands

Intentional Interference: Illegal Jammers

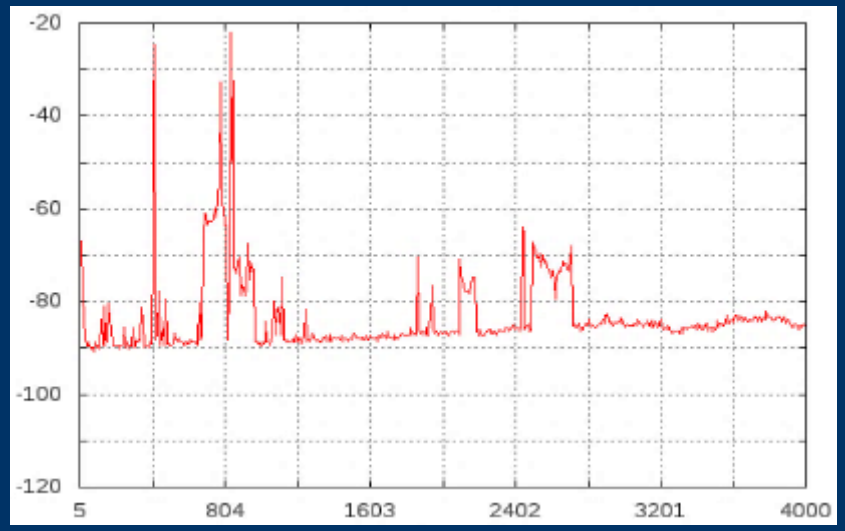
- **Manufacture**, **importation**, **marketing**, **sale** or **operation** of jamming devices is **ILLEGAL** in the United States (47 U.S.C. § 302a(B))
- It is also **ILLEGAL** to interfere with any licensed radio communications authorized by the FCC or operated by the U.S. Government (47 U.S.C. § 333)
- **Talk with your legal counsel about legal authorities available to your agency**, including any applicable state or municipal regulations
    - As appropriate, jamming incidents may be prosecuted as **interfering with police business** or as a **cybercrime**, in addition to jamming-specific charges

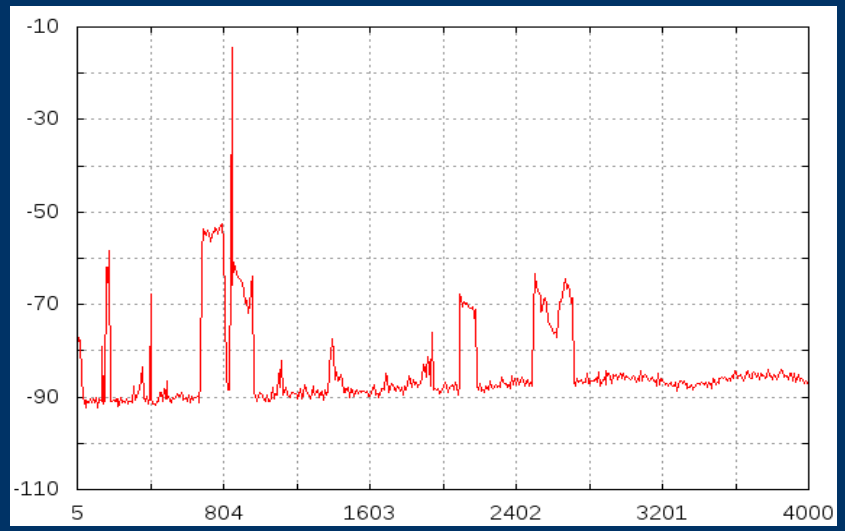
PRE-JAMMING



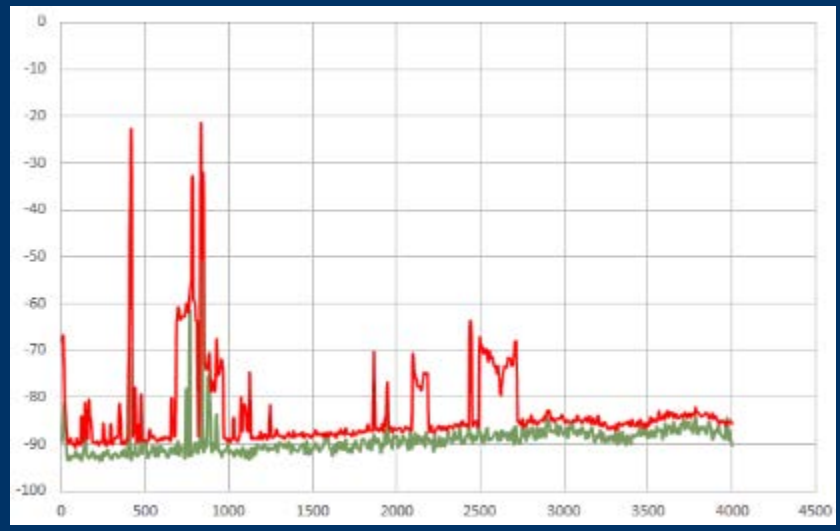


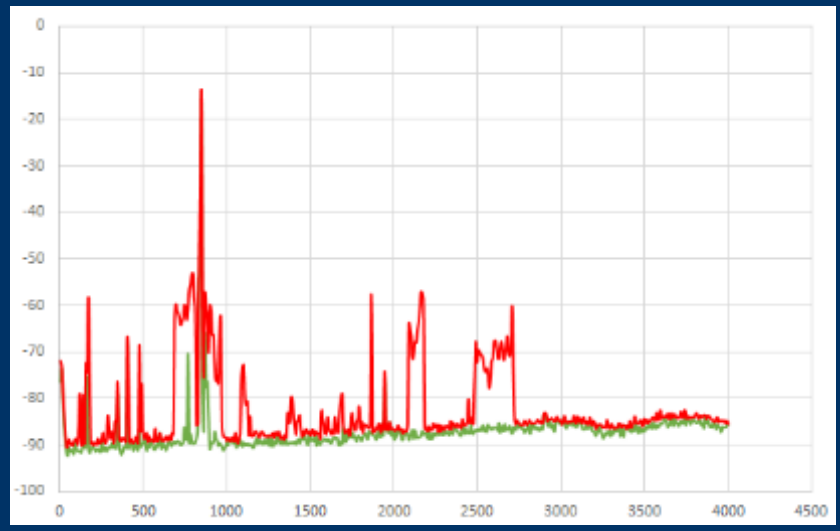
MID-JAMMING





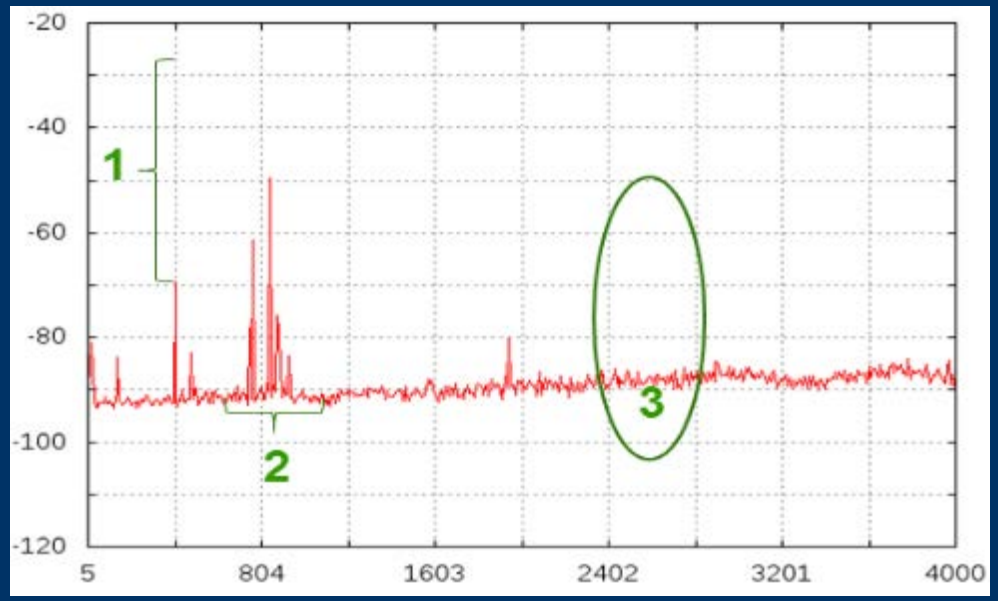
COMBINED



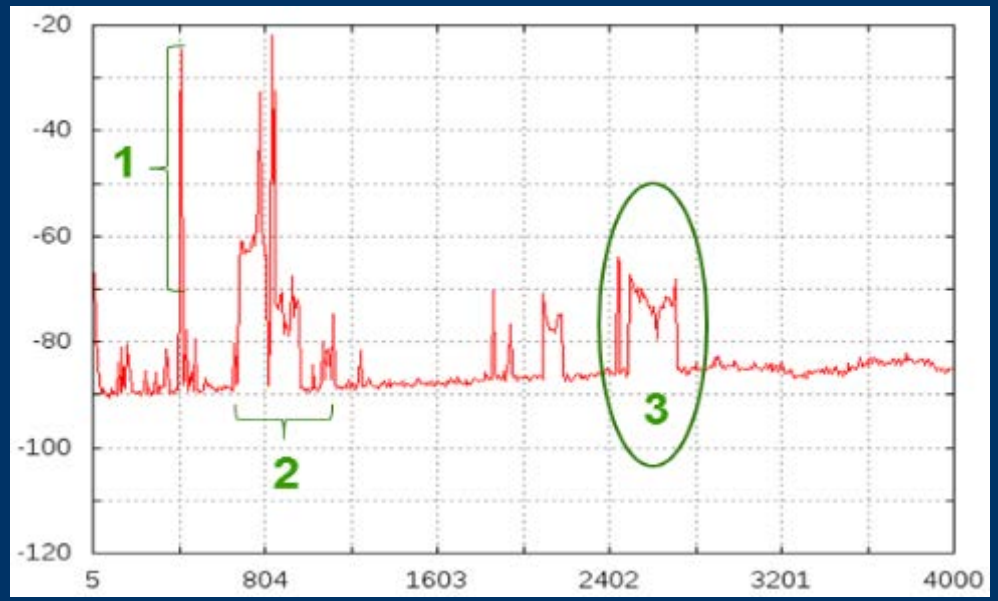


Key Spectrum Characteristics of Jamming

1. Signals have a higher power level than normal
2. There are large wide-bands of noise greater than normal operating bandwidth – normally LMR signals are narrowband
3. There may be signals in bands that are not used by your normal communications equipment – additional spurs or harmonics



PRE-JAMMING



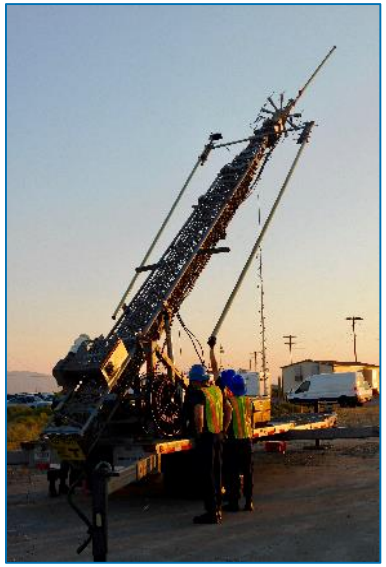
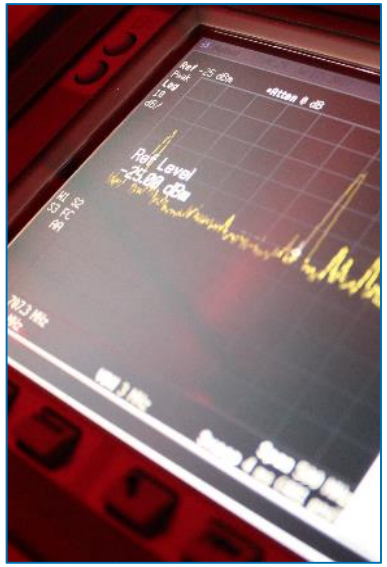
MID-JAMMING

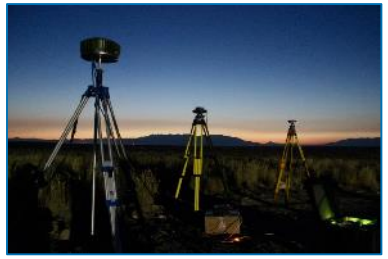
MITIGATING INTERFERENCE

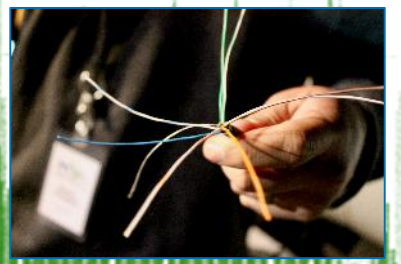
DHS Science & Technology Directorate's
First Responder Electronic Jamming Exercise

- The DHS 2016 First Responder Electronic Jamming Exercise tested illegal, commercial-grade jammers against public safety communications
- At JamX 17, DHS evaluated technologies and tactics that may help first responders identify, locate and mitigate jamming impacts
- DHS will publish a series of knowledge products for public safety, based on JamX 17 results
  - A full report will **not** be publicly posted due to sensitivities

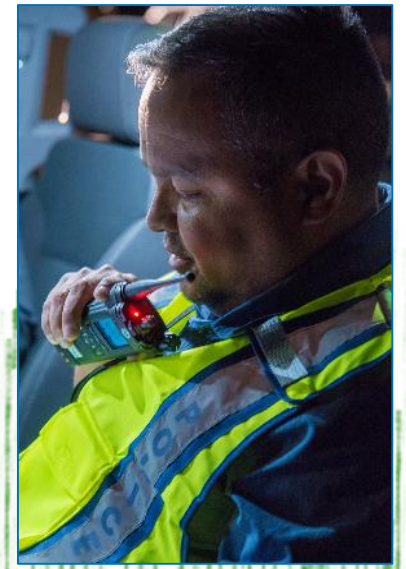
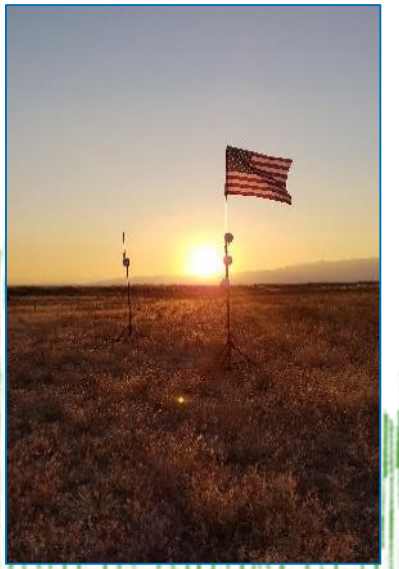
JAM X 17
FIRST RESPONDER
ELECTRONIC JAMMING EXERCISE




Ref Level
-25.00 dBm

JAM X 17
FIRST RESPONDER
ELECTRONIC JAMMING EXERCISE


Mitigating Jamming:
First Responder Perspective

- Communications failures are always assumed to be equipment issues
- Set operators up for success through equipment purchasing, setup and fleetmap management
- Education is key – operators must understand jamming threats to take them seriously
- Basic mitigation strategies include shielding and height

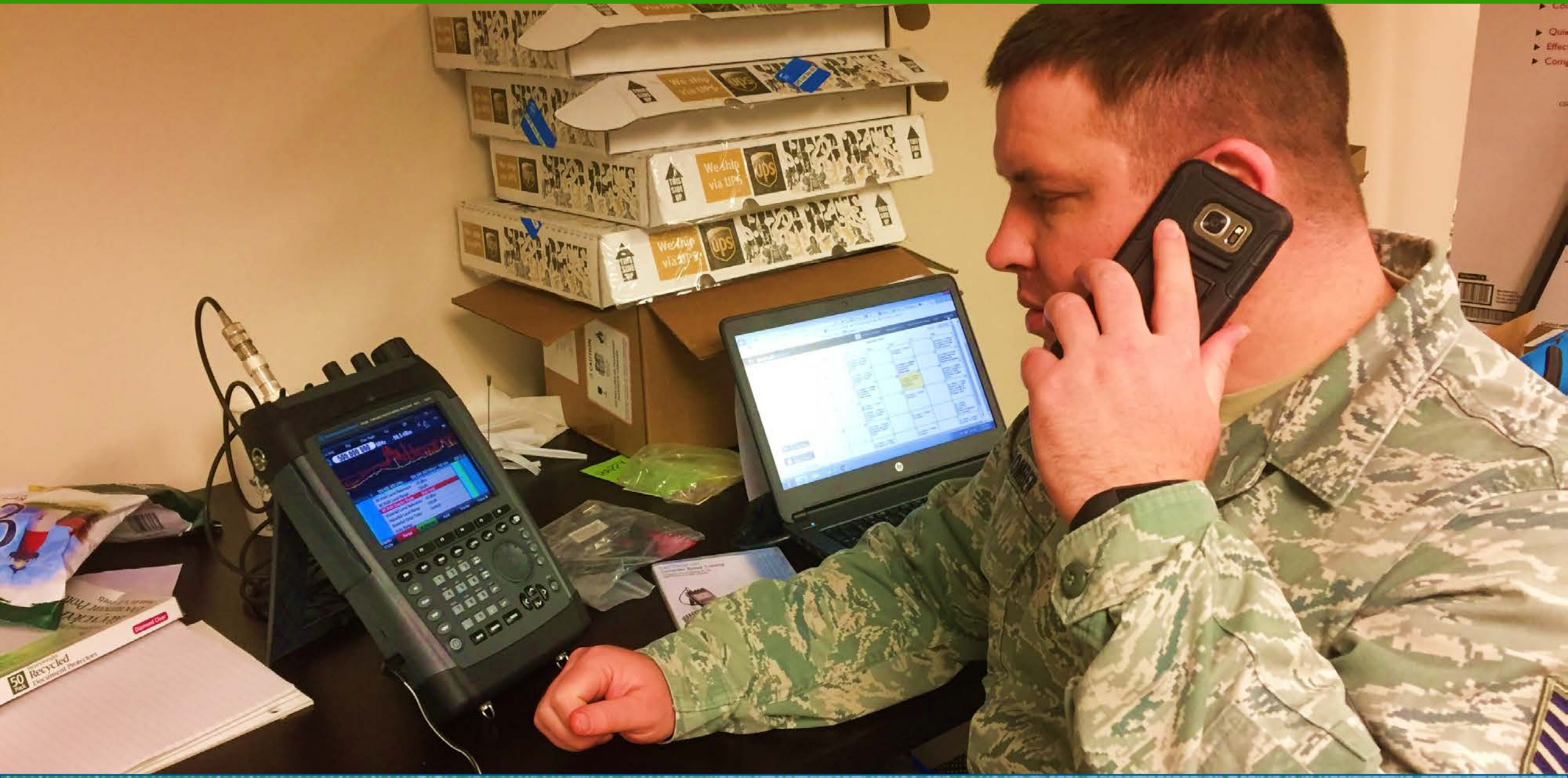
Mitigating Jamming:
Increasing Communications Resiliency

- Ensure all levels of organization are aware of jamming threats
- Consult organization’s legal counsel to understand state and local jamming laws
- Encourage regular radio training drills for operational personnel
- Have communications systems in multiple bands for backup
- Require prompt reporting of “equipment issues” to the communications team
- Switch on Automatic Gain Control in radio programing for all LMRs

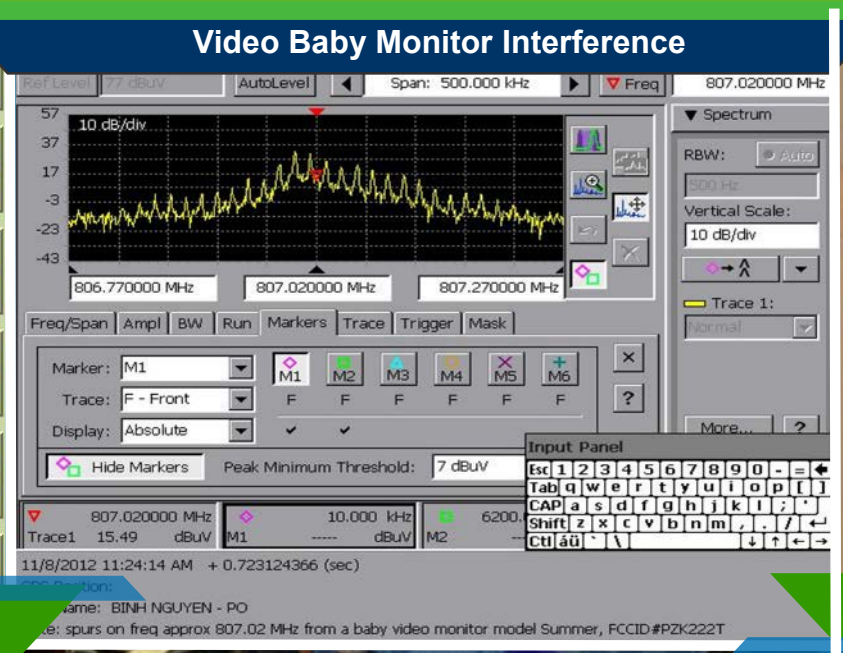
Mitigating Jamming:
Special Events

- Develop a PACE (Primary, Alternate, Contingency, Emergency) plan for communications
- Alert coordinating jurisdictions of potential jamming threats, symptoms and reporting procedures
- Train event security teams on jammer identification and mitigation tactics
- Monitor event with spectrum analyzers
- Use direction-finding tools to locate interference sources

CASE STUDIES

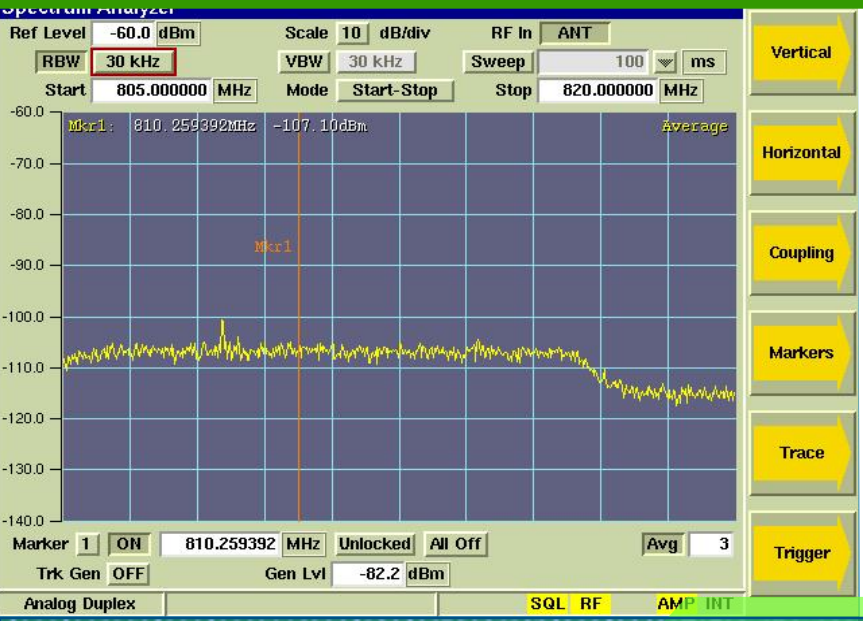

We Ship via UPS
UPS
Recycled

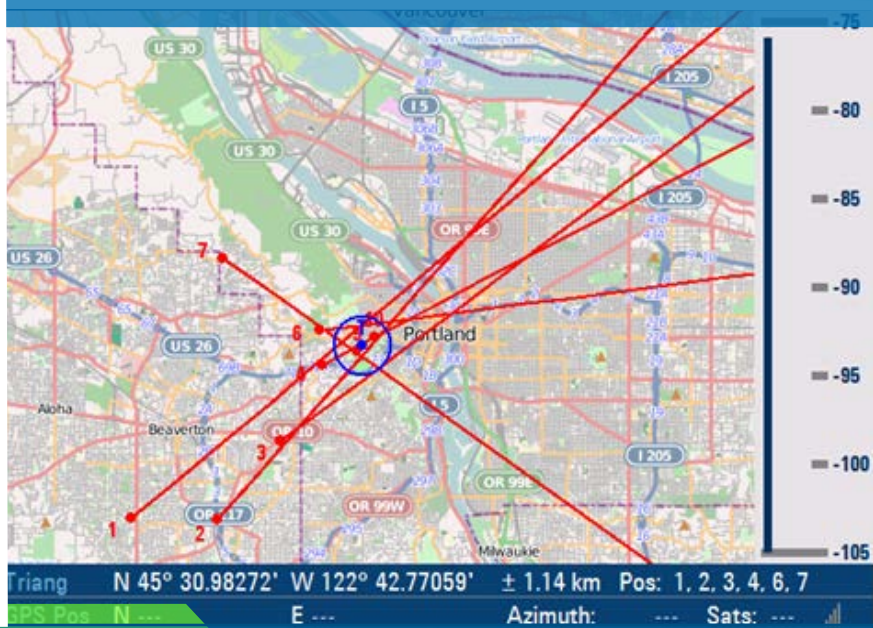
Video Baby Monitor Interference



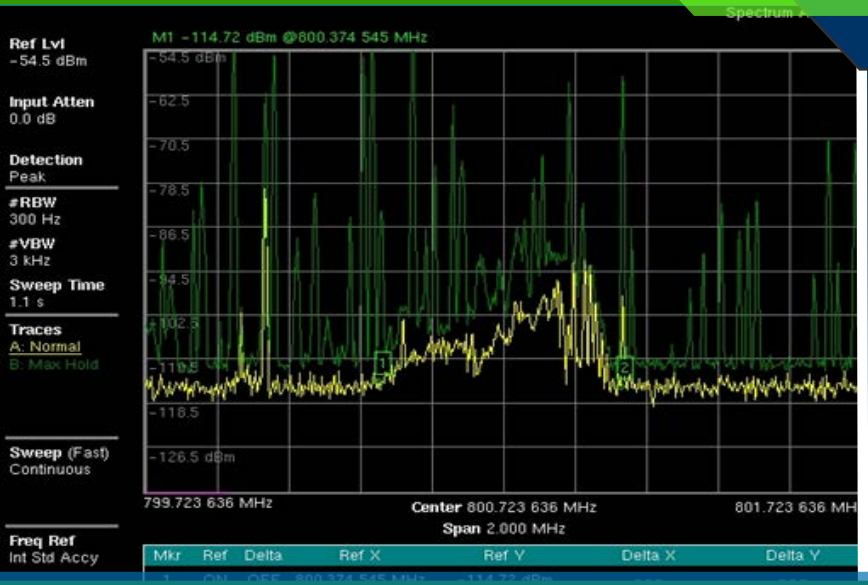
Defective BDA Interference

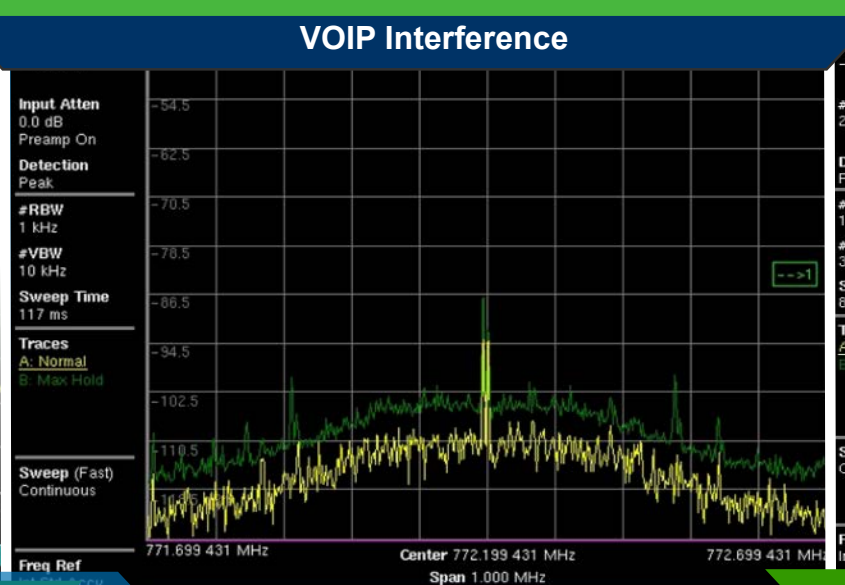
Quantar Receiver Blocking Interference

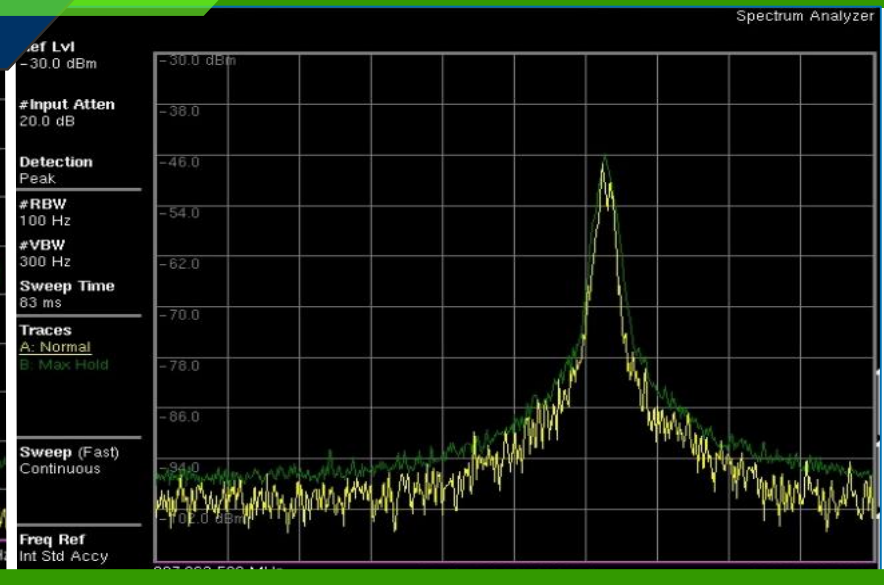




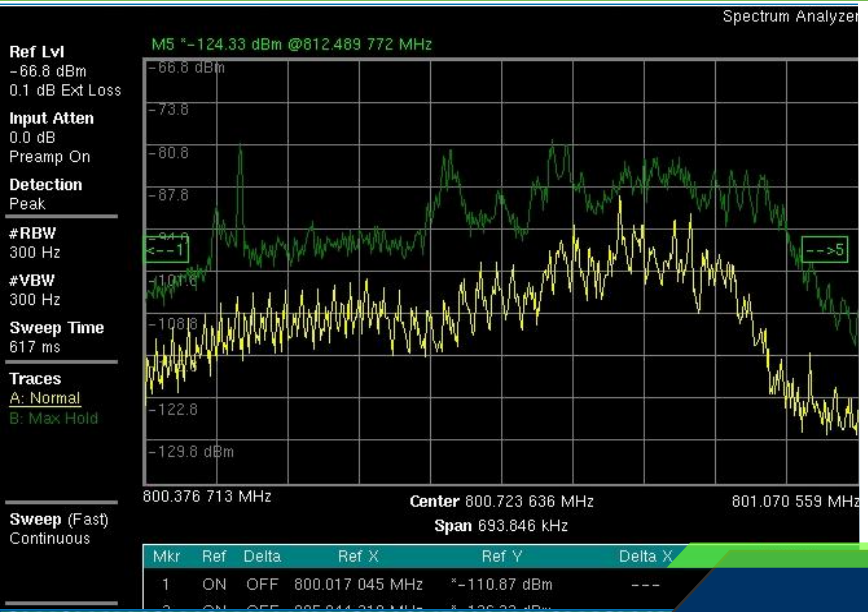
VOIP Interference

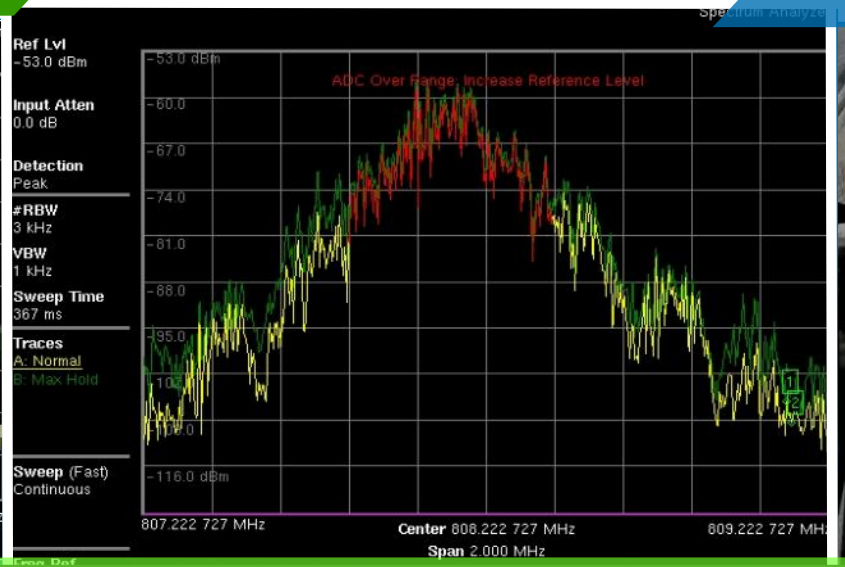






Baby Monitor Interference – Voice Uplink





Wireless Microphone Interference

Equipment Scanner Interference

Get Involved and Get Prepared

- Everyone has a responsibility for communications resiliency
- Raise awareness of jamming threats
- Implement recommendations to boost your communications resiliency
- Have a plan for what operators do when they suspect interference
- Talk to your legal counsel about state and local jamming laws
- If you See Something, Say Something - Report all suspected jamming incidents to the FCC

Reporting Jamming

- All suspected radio frequency interference **MUST** be reported to the Federal Communications Commission as soon as possible
- DHS and the FCC monitor reports of interference and jamming to conduct trend analysis and inform policy

CONTACT THE 24/7 FCC OPERATIONS CENTER

CALL
1-202-418-1122

EMAIL
FCCOPS@fcc.gov

WEBSITE
www.fcc.gov/general/public-safety-support-center

Engage With Us!

DHS S&T JAMMING EXERCISE PROGRAM

PRIMARY EMAIL
Jamming.Exercise@hq.dhs.gov

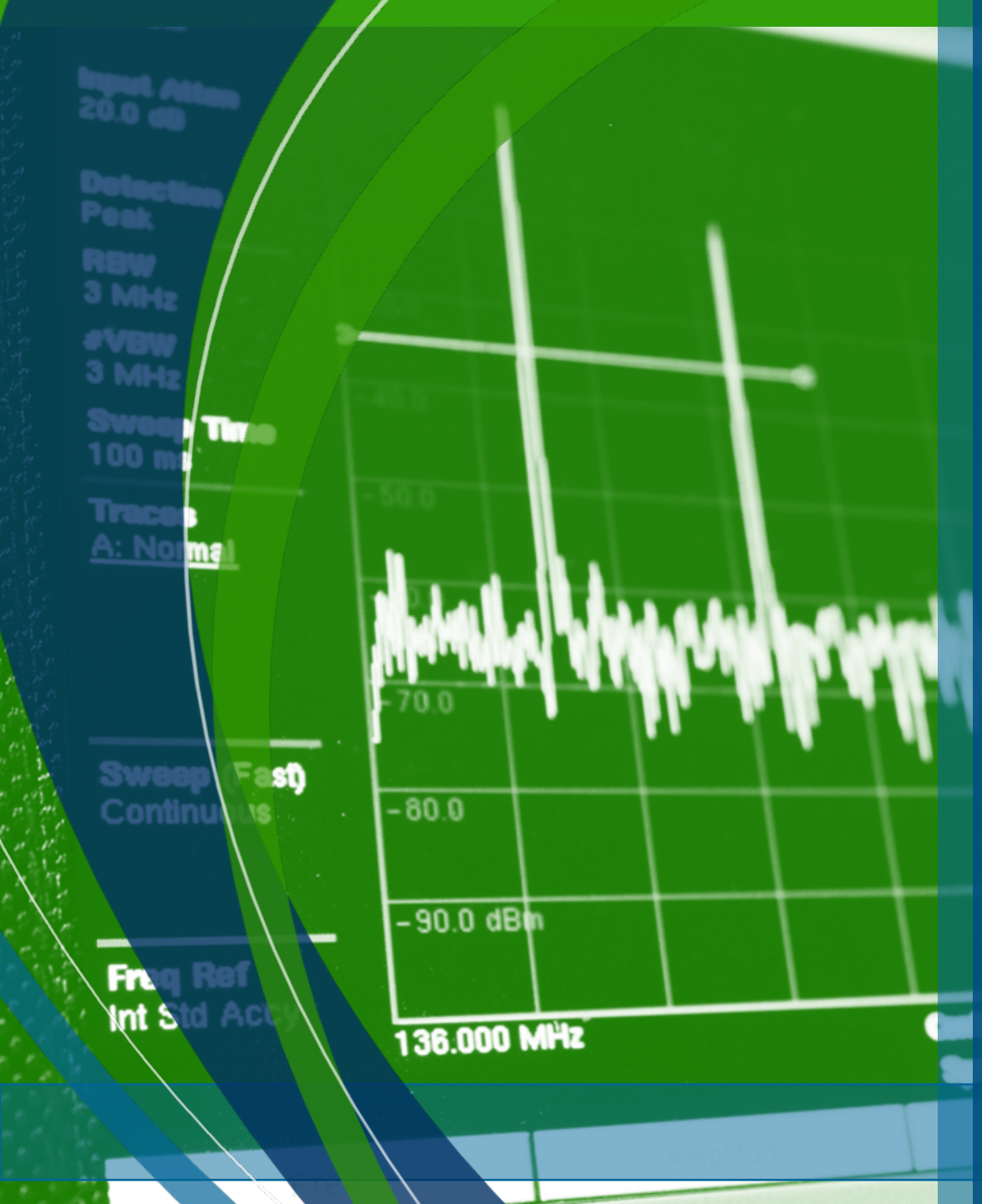
DHS S&T FIRST RESPONDERS GROUP

WEBSITE
www.FirstResponder.gov

TWITTER
@dhsscitech

EMAIL
First.Responder@dhs.gov

FACEBOOK
@FirstRespondersGroup AND @dhsscitech



THANK YOU
FOR JOINING US!

Homeland Security

Science and Technology