



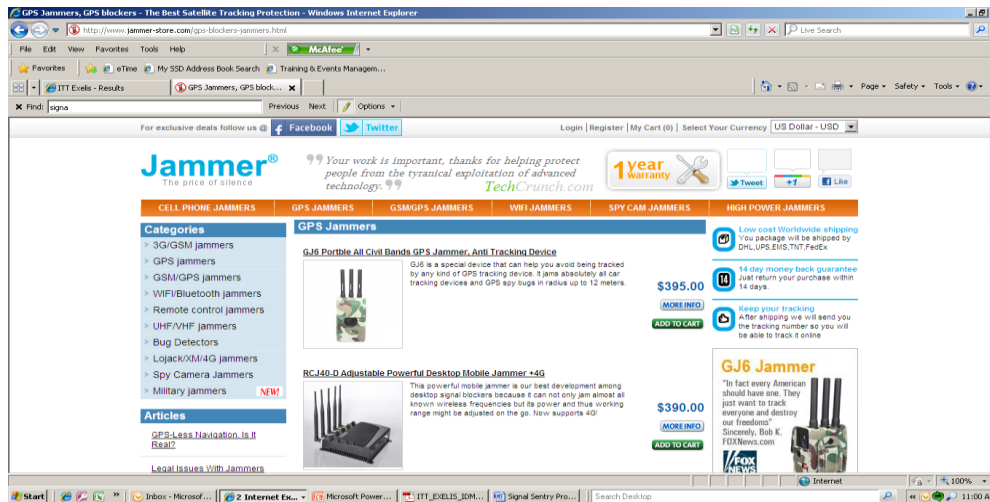
**GPS Interference Detection &
Geolocation Technology**
October 2015

Joe Rolli

Business Development

This document is not subject to the controls of the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

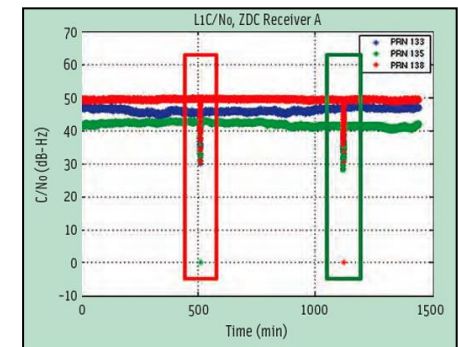
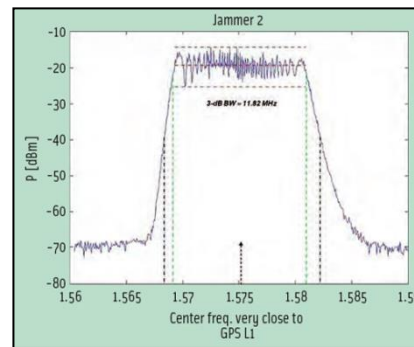
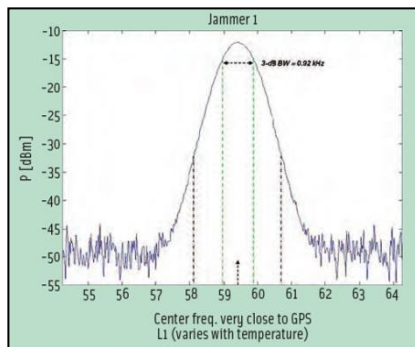
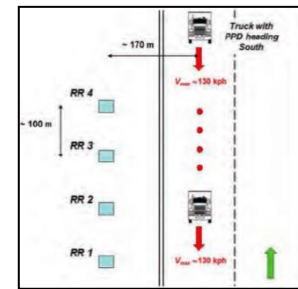
GPS susceptible to outages due to intentional & unintentional jamming
A small jammer can disrupt the GPS signal for a mile or more
People jam because they are smuggling, stealing or trying to escape tracking
Availability of low-cost GPS jamming devices has increased the risk



Real Risk of GPS Disruption

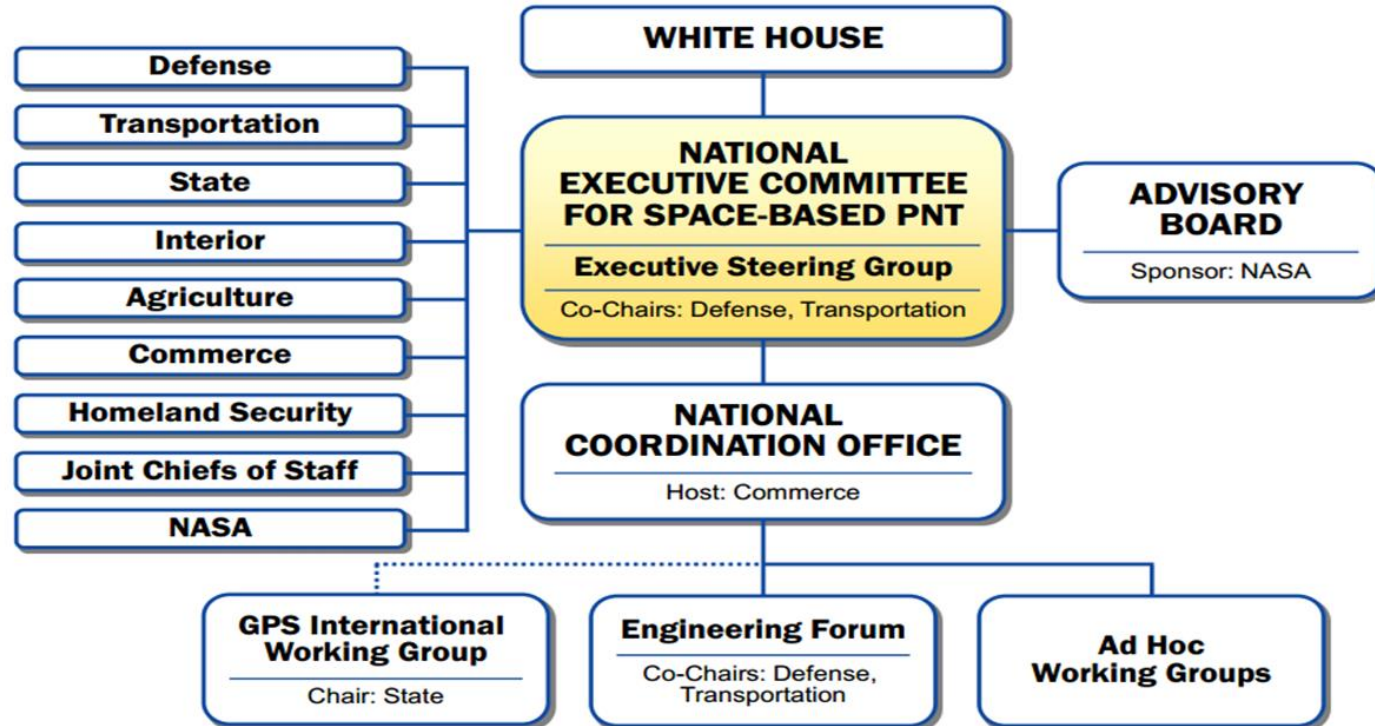


November 2009 Newark New Jersey
Ground-based Augmentation System (GBAS) Jammed
Took 8 months to find the source



PNT Advisory BD “We must quickly develop and field systems that will rapidly locate, mitigate and shutdown the interference”

U.S. Organizational Structure for GPS Governance



Summary: The United States is now critically dependent on GPS. For example, cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System (NEXGEN) cannot function without it. Yet we find increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations.

Most alarming, the very recent web availability of small GPS-Jammers suggests the problem will get worse. These so-called personal protection devices (PPDs) as well as other, readily available, more powerful devices can deliberately jam the Global Positioning System (GPS) signal over tens of square miles. They also can be devastating to the other, new foreign satellite navigation systems being deployed worldwide.

PPDs are illegal to operate, but many versions are available (for as little as \$30) from foreign manufacturers over the Internet. The simplest models plug in to a cigarette lighter and prevent all GPS reception within a line of sight range of 5 to 10 miles. Current penalty for operation is simply that the device is confiscated.

We currently lack sufficient capabilities to locate and mitigate GPS jamming. It literally took months to locate such a device that was interfering with a new GPS based landing system being installed at Newark Airport, NJ.

We must quickly develop and field systems that will rapidly locate, mitigate and shutdown the interference.

Real Risk of GPS Disruption Is Getting Worse



Home News Archive Events Jobs Market Reports Whitepapers & Media Supplier A-Z SUBSCRIBE Search

Pharma cargo thieves start to deploy jamming technology

Companies often deploy covert GPS-tracking technology in the fight against cargo theft, but thieves are now entering the arms race.

A series of attempted cargo thefts of pharmaceuticals being shipped by road have featured the use of jamming devices, deployed in an attempt to block the tracking signals and prevent security firms and the police recovering stolen shipments, according to the Pharmaceutical Cargo Security Coalition (PCSC).

Just last week, a tractor and trailer hauling \$2m-worth of pharmaceutical products was stolen from a truck stop in Cartersville, Georgia, with the thieves deploying two separate GSM jammers (pictured), but were unsuccessful. Law enforcement was able to track the shipment and recover the product intact, although those behind the theft evaded capture.

There was at least one portable tracking device, supplied by HIDEONTEC USA and monitored by GlobalTRIS, concealed within that shipment which ultimately assisted in guiding police officials to make the recovery, according to the PCSC. The vehicle's components

Phil Taylor
30-Jul-2014
Tweets 11
Shares 53
Print
Email Author

Related articles:

- Pharmaceutical crime: news in brief
- Pharmaceutical crime: news in brief
- Beyond quality: securing the supply of pharma ingredients
- Spikes in pharmaceutical thefts in 2013
- Disunion state approves bill to tackle cargo theft
- Product security: a growing concern for healthcare firms
- Man behind Lily warehouse burglary pleads guilty

Wine Track 2015
TRAÇABILITÉ - AUTHENTICITÉ - INTÉGRITÉ DES VINS ET SPIRITUEUX
PALAIS DES CONGRES DE BEAUNE - BOURGOGNE 13 MARS 2015

PHARMACEUTICAL TRACABILITY FORUM
14 - 16 April 2015



The FCC said an aircraft tracking system at Newark Liberty International Airport experienced interference from a GPS jamming device used by a Readington man who claimed he was simply trying to hide his whereabouts from his employer. The FCC fined the driver \$31,875 Aug 2012

Pharmaceutical Cargo Security Coalition Symposium * Novartis Pharmaceutical East Hanover February 10-11 2015

Forty-Six Stolen Luxury Cars Returned to Port of Los Angeles

InsuranceCrime
32,342

Published on Jun 19, 2013
Law enforcement officials at the Port of Los Angeles have uncovered a major organized criminal ring responsible for the theft and attempted exportation of over two million dollars worth of high-end vehicles.

46 Stolen Cars and exported from LA Port Using GPS PPD

Up Next

- The Real Hustle - The Car Dealer Can
- Woman who bought stolen car gets it back
- Car thieves make stolen cars legal
- Demo of how quickly a car can be rigged for parts
- Stolen Car Returned 30 Years Later And in Better Condition
- loading a car into a container atitanic style. Did they get it in ?
- How cars are stolen through OBD port theft and key cloning

IN HOMELAND SECURITY
News & Analysis of Critical Issues in Terrorism & Homeland Defense

Home About the Blog Categories Contributors Partnerships Newsletter Blogro

GPS Jammers, Other Maritime Cyber Security Threats Discussed At Seminar
March 3, 2015

Vice Adm. Chuck Michel, USCG, addressing the Seminar and Symposium on Maritime Cyber Security

By Glyn Cosker
Managing Editor, In Homeland Security

The Learning Seminar and Symposium on Maritime Cyber Security, co-sponsored by Rutgers University and American Military University (AMU) enters its second day today on the campus of Rutgers University, New Brunswick, N.J.

Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) and AMU are hosting the event that covers a wide range of maritime cyber security issues, national security and data breaches. The seminar features several keynote speakers from the U.S. military, homeland security coverage: control/defense/2015/13/maritime-security-seminar/13/assured-communications

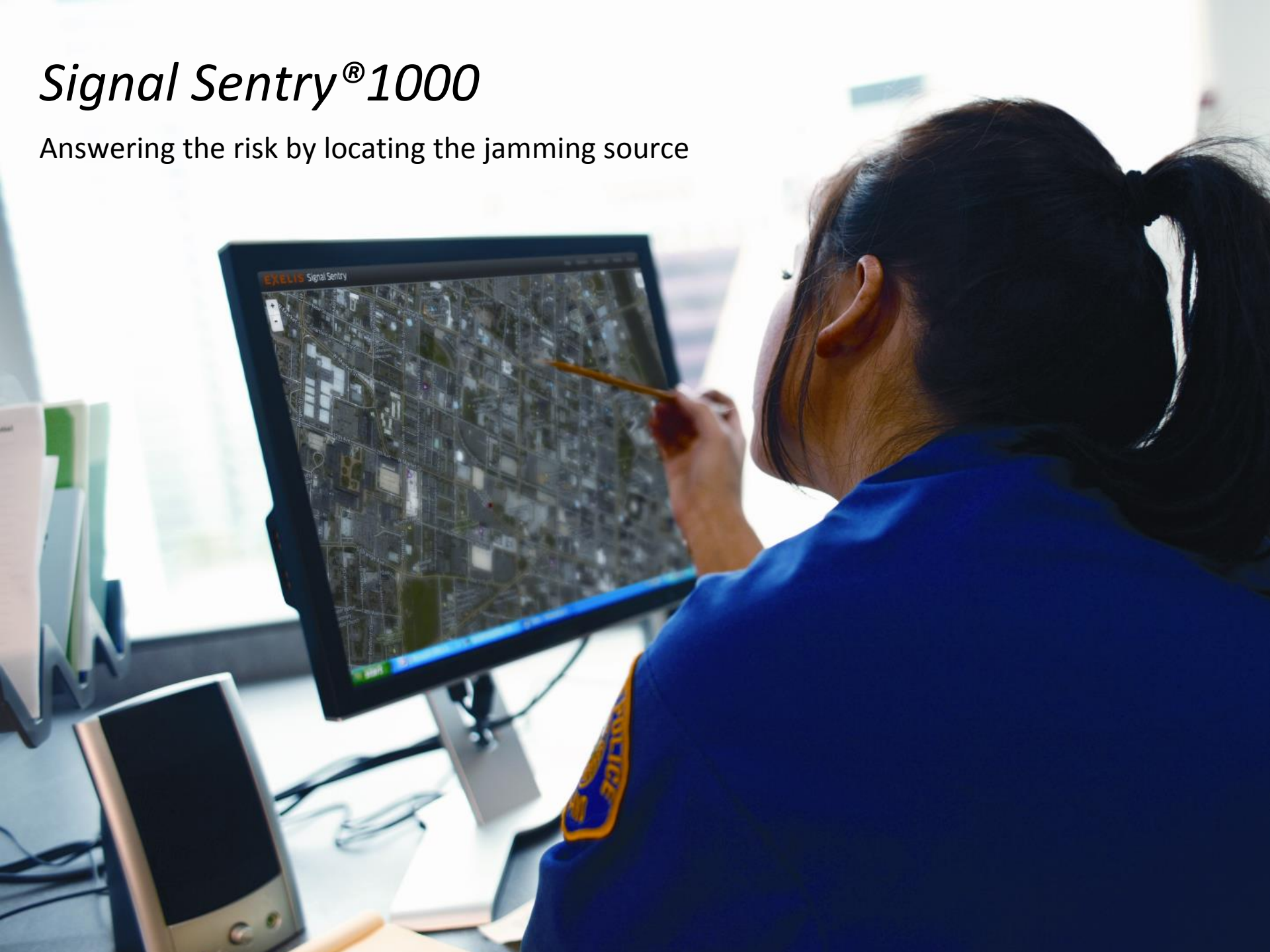
Coast Guard Vice-Admiral Chuck Michel saw it happen in one Eastern Seaboard port.

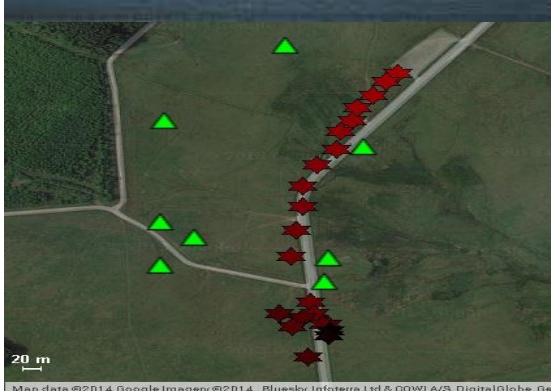
"It was believed to be sort of a vandal or a person messing around, actually blocked that GPS signal from that computer's ability to do that, and the port came to a halt," he said.
*Maritime Cyber Security Symposium
March 2-3 2015



Signal Sentry[®] 1000

Answering the risk by locating the jamming source





Signal Sentry

- Designed to protect critical infrastructure from GPS disruption jamming & spoofing
- Situational Awareness of GPS Interference
- Real time geolocation of GPS interference
- Actionable Intelligence for quick mitigation of GPS disruption

Deployed Systems

- 2014 Super Bowl at Met Life Stadium
- Southampton Port United Kingdom
- Newark N.J DHS & Essex County Sherriff

Field Tested

- Sennybridge Test Range UK
- Vidsel test range in Sweden

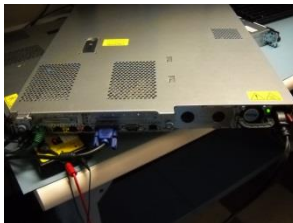
Includes antennas, sensors and a server

- Each Sensor has two antennas
- Sensors are connected to either a local or cloud-based server

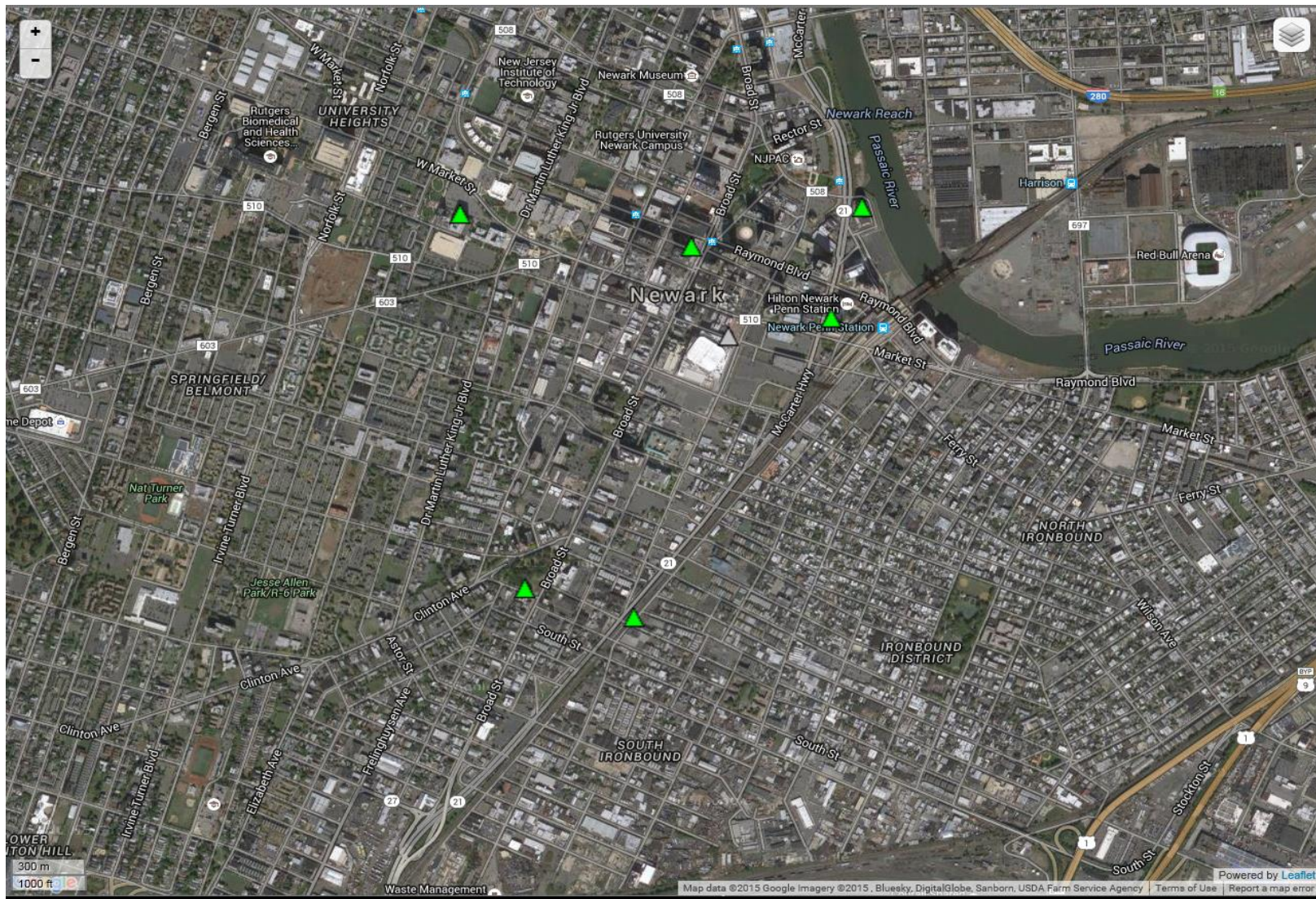
System detects, locates and maps the jamming source

Data is available through an easy-to-use web enabled GUI

Information used for action – change navigation methods, alert authorities...



Signal Sentry Home Page Newark NJ



*This document is not export controlled.
Use or disclosure of this information is
subject to the restrictions on the Title
Page of this document.*

Sensor Location



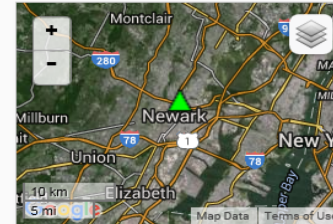
Sensors

Name	Configured Address/Port	Reported Address	Status	Interference State	Event Started
sw200403 - Essex County Sheriff: FBI Building	71.250.253.59:12623	71.250.253.59	Registered	No Event	N/A
sw200464 - Essex County Sheriff: Salvation Army	71.250.253.60:12623	71.250.253.60	Registered	No Event	N/A
sw200470 - Essex County Sheriff: Integrity House	71.250.253.61:12623	71.250.253.61	Registered	No Event	N/A
sw200474 - Essex County Sheriff: Prudential Center	166.249.121.42:12623	166.249.121.42	Communication Fault	Unknown	N/A
sw200478 - Essex County Sheriff: Prudential Building	166.249.121.29:12623	166.249.121.29	Registered	No Event	N/A
sw200486 - Essex County Sheriff: Court House	71.250.254.137:12623	71.250.254.137	Registered	No Event	N/A
sw200487 - Essex County Sheriff: One Gateway	71.250.242.196:12623	71.250.242.196	Registered	No Event	N/A

sw200403 - Essex County Sheriff: FBI Building

Sensor Info

Interference State	No Event
Sensor Status	Registered
GPS Fix Status	Has GPS fix
Configured Latitude	40.73820702
Configured Longitude	-74.1645826
Configured Geoid (MSL) Altitude (m)	64.567
GPS-Reported Latitude	40.7381801
GPS-Reported Longitude	-74.16459790000002
GPS-Reported Geoid (MSL) Altitude (m)	57.182
Configured Address/Port	71.250.253.59:12623
Reported Address	71.250.253.59
Last Application Ping	9/24/2015 2:39:55 PM
Last Position Report	9/24/2015 2:39:51 PM
FFT Processing	Healthy
Firmware Version	2.18.01
GPS Version	CTL414V05 rev 2.15



Lat: 40.7382 Lon: -74.1646

Geoid (MSL) Alt: 64.5670 m

[GPS DOP/TACC](#)

[GPS Quickthresh](#)

[GPS Satellites](#)

[GPS Multipath by Azimuth](#)

[GPS SNR by PRN](#)

[Sensor Log](#)

[Raw Data](#)

[Event Frequency](#)

[Interference Settings](#)

[SNR Settings](#)

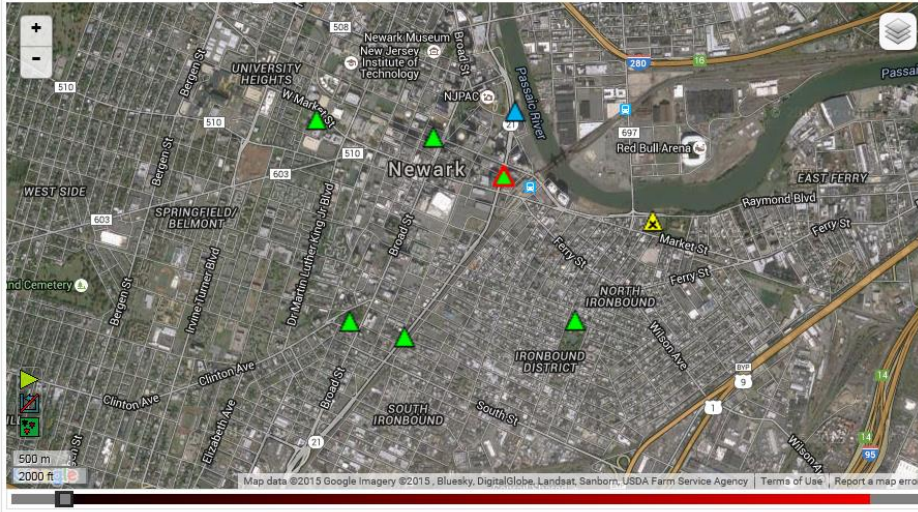
[GPS Settings](#)

[Position Override Settings](#)

[Unregister Sensor](#)

Interferer Details

Interferer Map



Interferer Details

Interferer Map



Essex County College Center for Technology

Interferers

Interferer Frequency Chart

Min. Interference Duration (hh:mm:ss) : :

- Show only Geolocated Interferers
- Show only Non-geolocated Interferers
- Show all Interferers

[Update](#)

Geolocated Interferers Lasting at Least 2 Hours

Interferer	Interference Duration (hh:mm:ss)	Interference Ended
Ended event started 10/20/2014 9:51:26 AM	2:31:17	10/20/2014 12:22:43 PM

Displaying interferers 1-1

Interference Frequency Events > 5 Min



Interferers

Interferer Frequency Chart

Min. Interference Duration (hh:mm:ss) : :

- Show only Geolocated Interferers
- Show only Non-geolocated Interferers
- Show all Interferers

Update

Geolocated Interferers Lasting at Least 5 Minutes

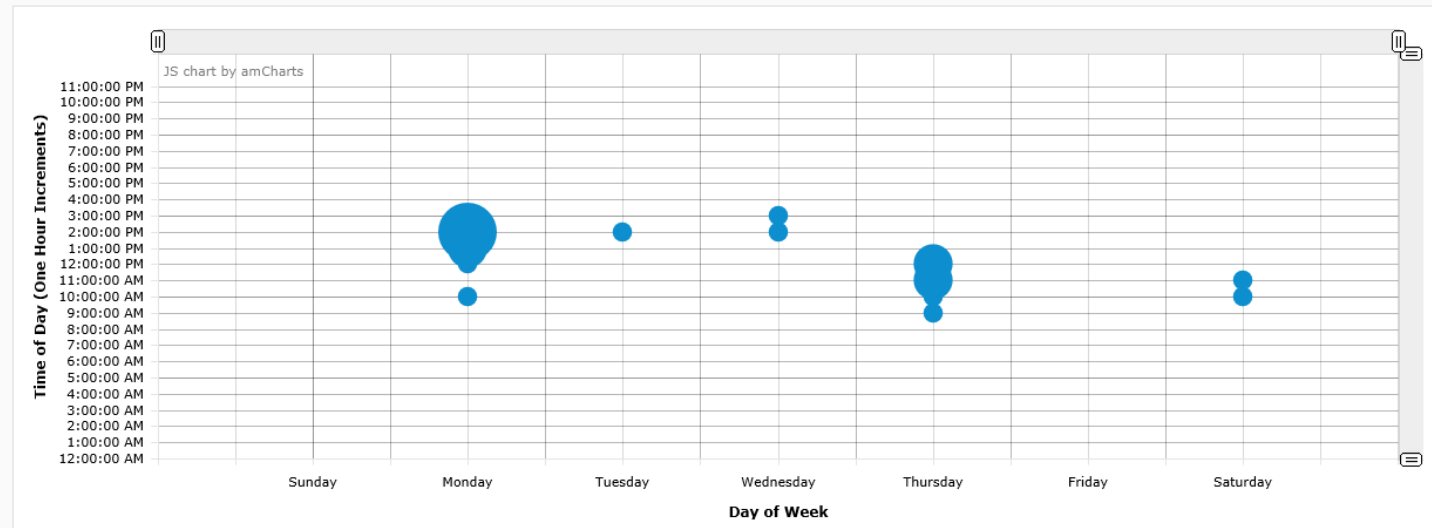
Interferer	Interference Duration (hh:mm:ss)	Interference Ended
Ended event started 6/16/2015 2:07:07 PM	0:11:42	6/16/2015 2:18:49 PM
Ended event started 6/11/2015 9:43:00 AM	0:05:44	6/11/2015 9:48:44 AM
Ended event started 5/11/2015 2:58:29 PM	0:56:16	5/11/2015 3:54:45 PM
Ended event started 4/30/2015 12:18:59 PM	0:07:30	4/30/2015 12:26:29 PM
Ended event started 4/30/2015 11:21:06 AM	0:10:28	4/30/2015 11:31:34 AM
Ended event started 4/30/2015 10:19:01 AM	0:39:22	4/30/2015 10:58:23 AM
Ended event started 4/27/2015 12:01:48 PM	1:24:00	4/27/2015 1:25:48 PM
Ended event started 3/30/2015 10:20:44 AM	0:12:46	3/30/2015 10:33:30 AM
Ended event started 3/16/2015 2:29:07 PM	0:15:15	3/16/2015 2:44:22 PM
Ended event started 3/16/2015 2:10:00 PM	0:18:28	3/16/2015 2:28:28 PM
Ended event started 3/16/2015 1:22:09 PM	0:13:15	3/16/2015 1:35:24 PM
Ended event started 1/28/2015 1:46:58 PM	0:19:07	1/28/2015 2:06:05 PM
Ended event started 1/24/2015 9:04:08 AM	1:23:12	1/24/2015 10:27:20 AM
Ended event started 1/8/2015 10:47:07 AM	0:24:10	1/8/2015 11:11:17 AM

When Events Occur



Interferer Frequency

Geolocated Instances of Interference Lasting at Least 5 Minutes by Day of Week / Time of Day (One Hour Increments) From 1/1/2015 3:08:01 PM To 9/24/2015 3:08:01 PM



If the option *Count only Geolocated Interferers* is enabled, clicking chart items causes a map to be displayed in this area that shows the geo-located interferers pertaining to the selected chart items. Selected chart items are shown in red, and non-selected chart items are shown in blue.

Resolution ▼

Min. Interference Duration (hh:mm:ss) : :

- Count only Geolocated Interferers
- Count only Non-geolocated Interferers
- Count all Interferers

From Date (MM/dd/yyyy hh:mm:ss) To Date

From Time of Day (hh:mm:ss) : : ▼

To Time of Day (hh:mm:ss) : : ▼

Email Alert Notification



Sign up for E-Mail or Text Message Notifications

Notifications will be sent from IDGSS@somedomain.com

Existing E-Mail/SMS Address(es)

	Address	Notify on Interference Event Detections	
		Duration	Geolocation Only
<input checked="" type="checkbox"/>	2013213816@vtext.com	0:15:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Brian.Flynn@exelisinc.com	0:00:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	jennie.womble@exelisinc.com	0:01:00	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	joseph.rolli@exelisinc.com	0:05:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	josh.magner@exelisinc.com	0:05:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Kevin.W.Stone@ice.dhs.gov	0:10:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	mitchell.erickson@HQ.DHS.GOV	0:05:00	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	monty.graham@hq.dhs.gov	1:00:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	raymond.ciaccio@dhs.gov	0:10:00	<input type="checkbox"/>
<input checked="" type="checkbox"/>	sarah.mahmood@dhs.gov	0:20:00	<input type="checkbox"/>



E-Mail/SMS Address(es)



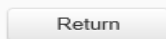
Send Notifications on Interference Event Detections



Geolocation Only



Duration of Event for Notifications (hh:mm:ss)



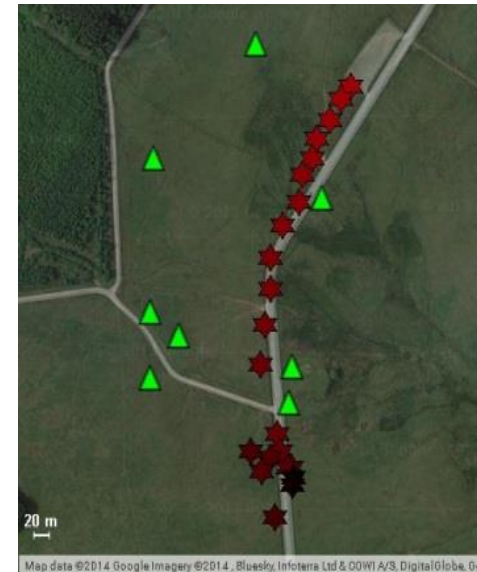


Map data ©2014 Google Imagery ©2014, Bluesky, DigitalGlobe, Sanborn, USDA Farm Service Agency - Terms of Use Report a map error

Signal Sentry 1000 Test Results



- Tested during GPS jamming trials in Sennybridge, UK in September 2014
- Trials administered by the Defence Science and Technology Laboratory
- Off-the-shelf jamming devices were used during the tests
- Located stationary & moving jammers in open & obstructed environments
- Jammers in a moving vehicle scenario were located with an average accuracy of 10 meters



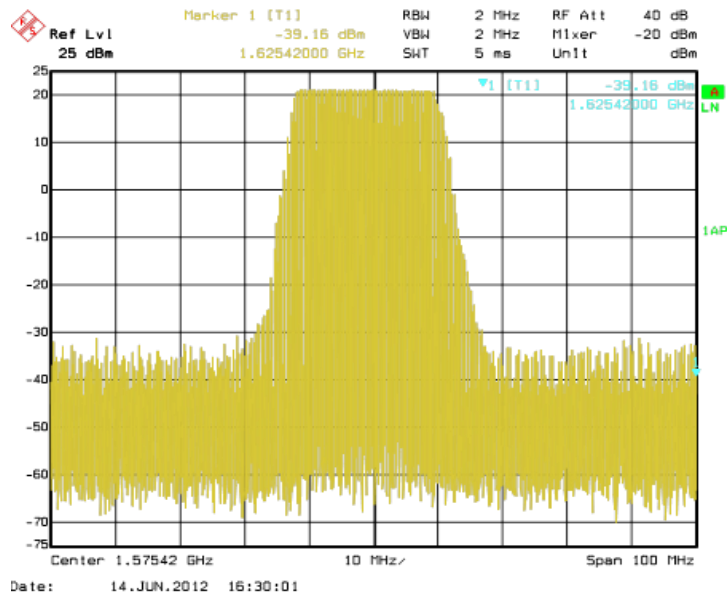
Jammer in car at 40 mph

Jammer Description

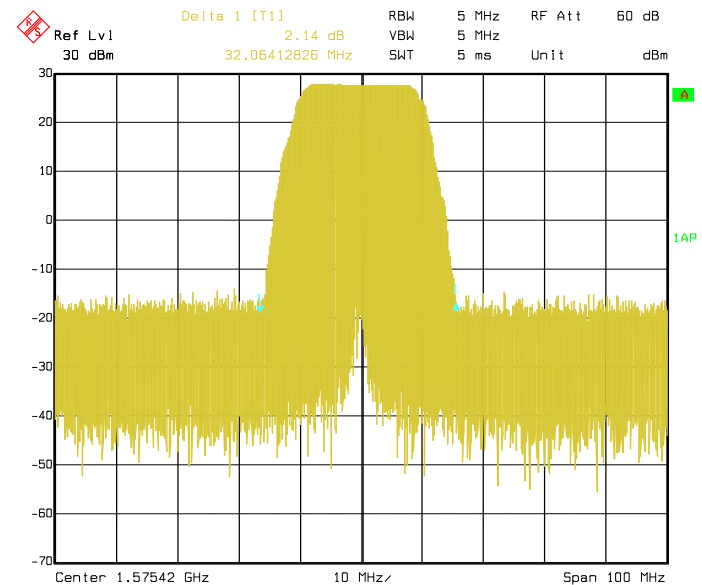


Two Jammers utilized during the trials
150mW and .5W

Used to disrupt the GPS L1CA code that operates at 1575.42 MHz

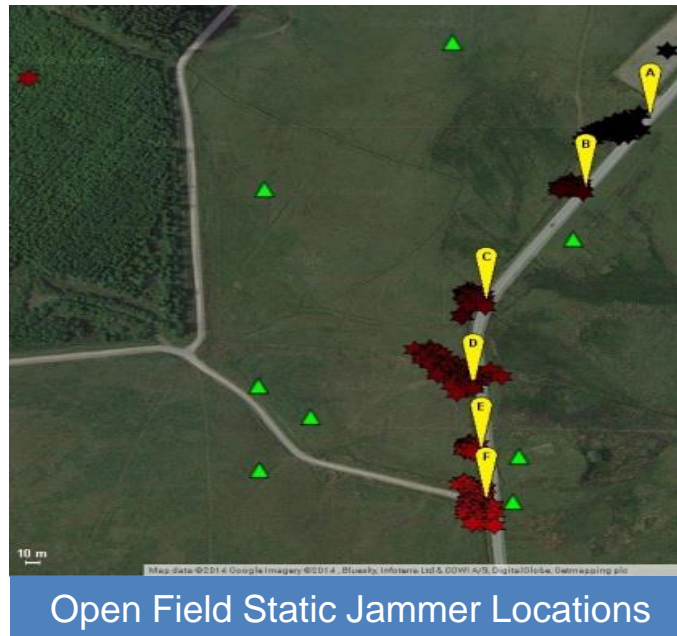


150mW jammer waveform



.5w jammer waveform

Test was constructed to geolocate jamming in an area with no obstructions
Test included static jammers and dynamic jammers
Six waypoints were surveyed for the purpose of evaluating location accuracy



- **GPS Interference events occur on average of ~4 a month in Newark**

- **Law Enforcement Essex County Sheriff & NY/NJ Port Authority Police**
 - **Not illegal to possess a GPS Jammer & can't prosecute**
 - **Most officers won't recognize GPS Jammer Devices**
 - **Recommended State & Local legislation to make possession of Jammers Illegal**
 - **“ Should not refer to them as Personal Privacy Devices they are Jammers”**

- **Jammers used by thieves to steal cargo put ports at risk of GPS disruption**
 - **Pharmaceutical Cargo Security Coalition Symposium**
 - **46 Stolen Cars exported from LA Port found with GPS Jammers**
 - **DHS Maritime Cyber Security Symposium Port came to halt GPS signal was blocked**

- **Testing this technology in a real environment is challenging due to very limited opportunities to use live GPS jammers**



For more information visit:
www.exelisinc.com/signalsentry