

Exelis Inc., a wholly owned subsidiary of Harris Corporation



Signal Sentry GPS Interference Detection June 2015

Joe Rolli

Business Development Manager

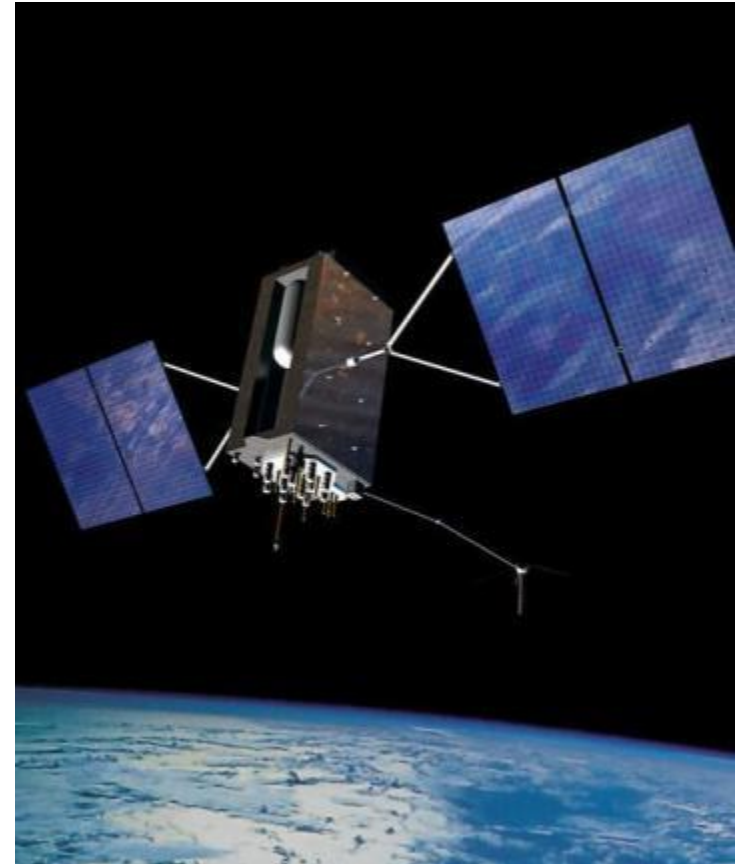


This document is not subject to the controls of the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

harris.com

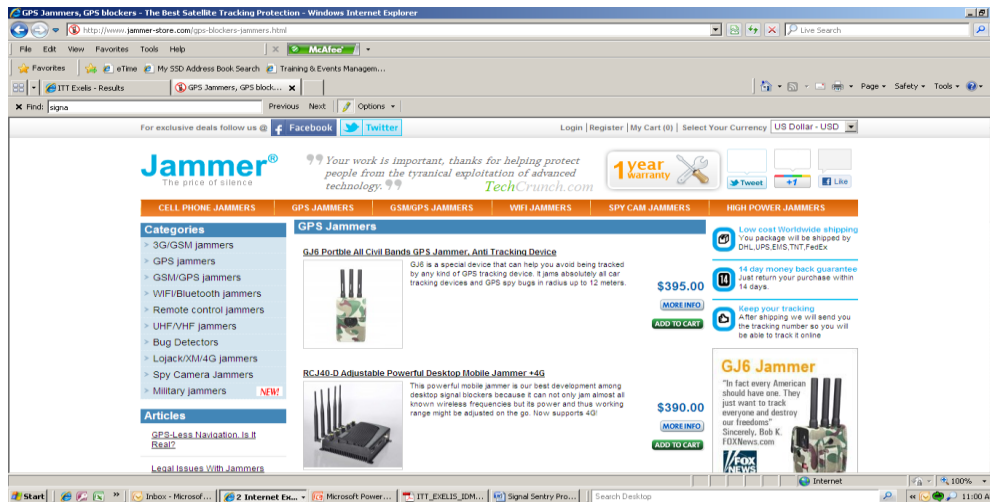
assuredcommunications® | Harris Proprietary Information

- **Exelis is the GPS Expert**
 - Developed Over 50 GPS satellite payloads
 - Payloads & Transmitters have been on every GPS satellite ever launched
 - Our payloads transmit the GPS signal from space
 - We have accumulated over 500 years of on-orbit life
 - No mission-related failure due to our equipment
 - Currently developing the next generation navigation payloads



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

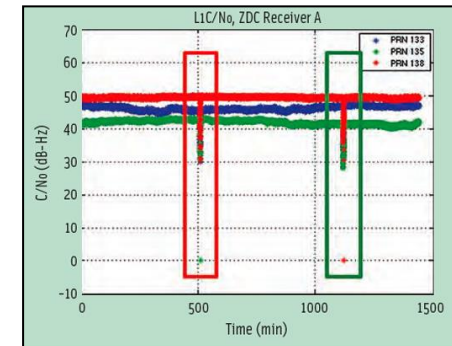
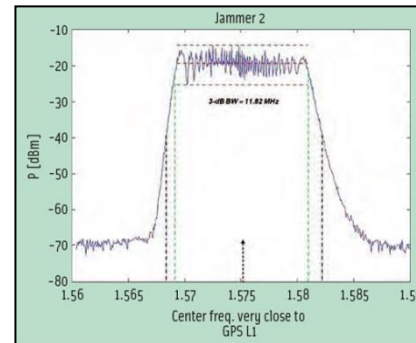
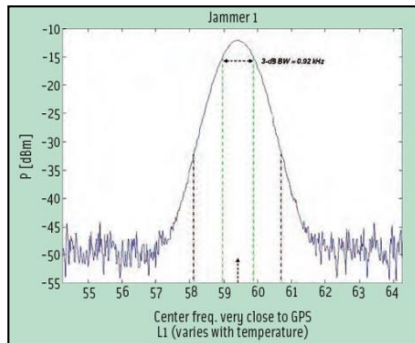
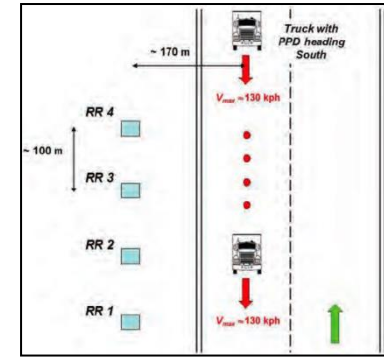
- > GPS jamming does not allow receivers to lock onto the GPS signal
- > GPS susceptible to outages due to intentional & unintentional jamming
- > A small jammer can disrupt the GPS signal for a mile or more
- > People jam because they are smuggling, stealing or trying to escape tracking
- > Availability of low-cost GPS jamming devices has increased the risk



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

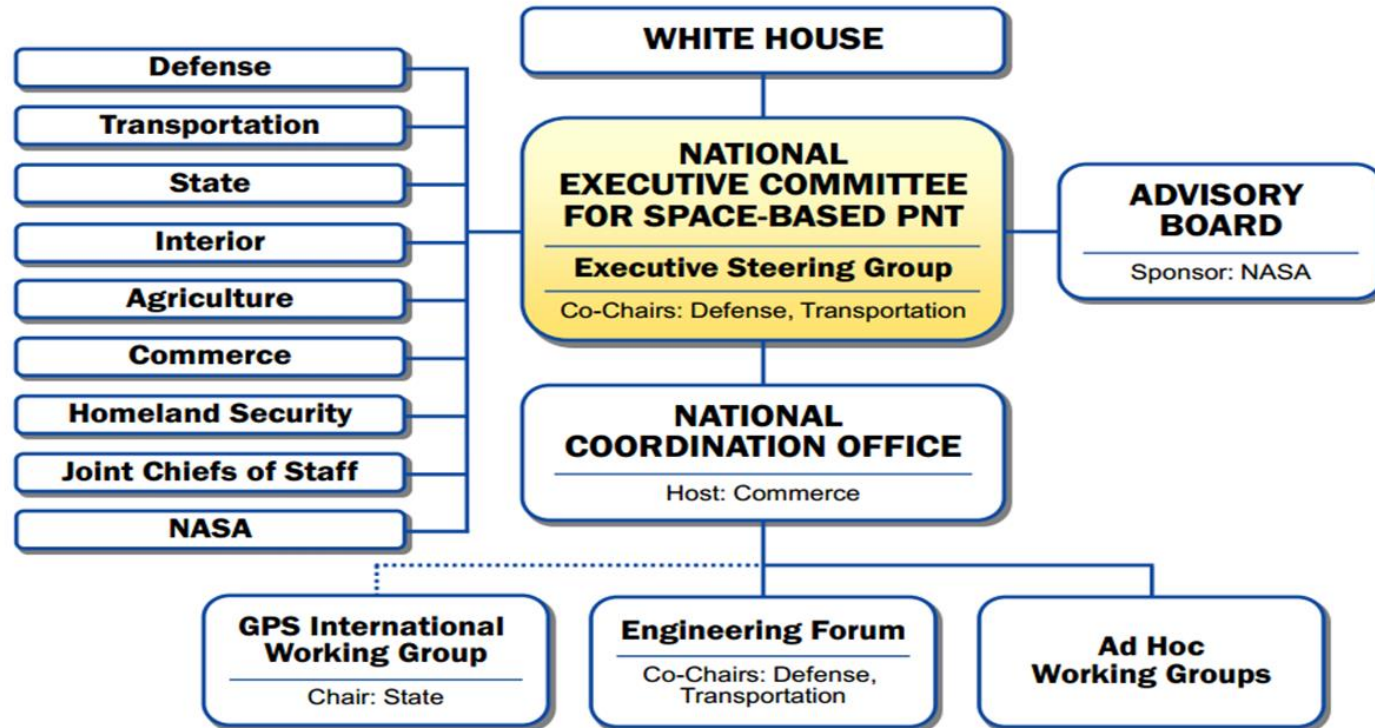
Real Risk of GPS Disruption

- November 2009
- Ground-based Augmentation Systems (GBAS) Jammed
- Took 8 months to find the source



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

U.S. Organizational Structure for GPS Governance



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

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




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

Pharmaceutical Food & Beverage Electronics & Industrial Cosmetics & Personal Care Clothing & Accessories Security Documents & IT

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.



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 HIDEHTEC 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 theft's discovery

Phil Taylor
30-Jul-2014

Tweet 11
Share 53
Print
Email Author

Related articles:

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

Wine Track 2015
TRACABILITE - AUTHENTICITE - INTEGRITE DES VINS ET SPIRITUEUX
PALAIS DES CONGRES DE BEAUNE - BOURGOGNE
15 MARS 2015

PHARMACEUTICAL TRACEABILITY FORUM
14-15 April 2015

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

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

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 hijacked for parts
- Stolen Car Returned 30 Years Later And in Better Condition
- loading a car into a container african style. Did they get it in 7
- How cars are stolen through OBD port theft and key cloning

IN GPS Jammers and Maritime Cyber Security Threats Discussed At Seminar

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

Home About the Blog Categories Contributors Partnerships Newsletter Blog

GPS Jammers, Other Maritime Cyber Security Threats Discussed At Seminar

March 3, 2015



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

By Glynn 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,



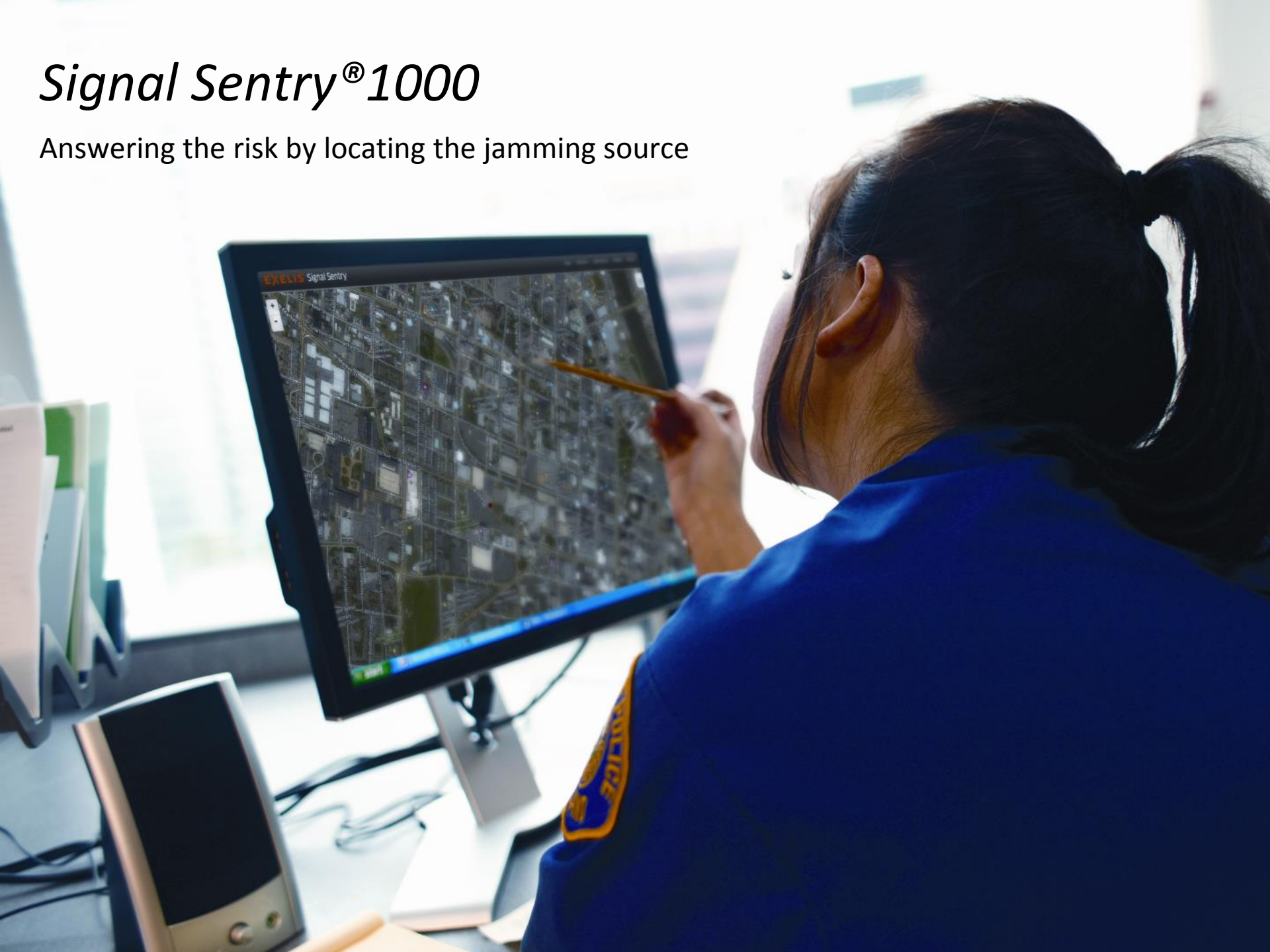
Coast Guard Vice-Admiral Chuck Michel saw it happen in one Eastern Seaboard port.

“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

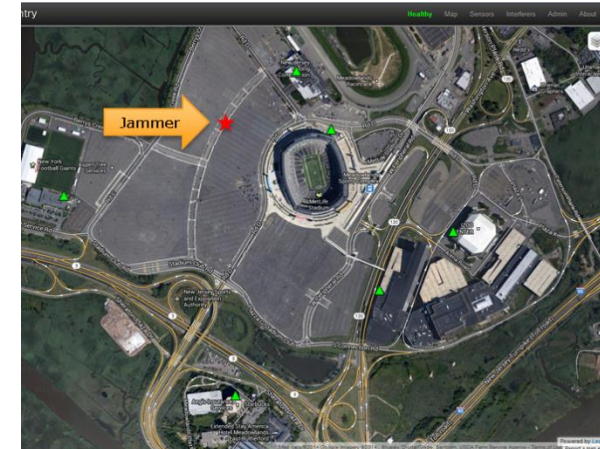
This document is not export controlled. Use or disclosure of this information is subject to the restrictions on the Title Page of this document.

Signal Sentry[®] 1000

Answering the risk by locating the jamming source

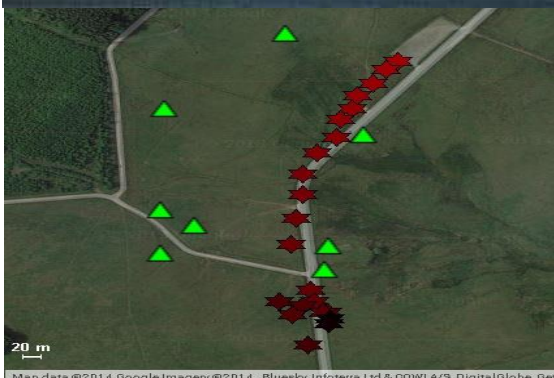


- > Detects and locates sources of GPS signal interference
- > Provides location of interference
- > Presented in the form of geographical pin mapping
- > Provides actionable intelligence to the user
- > Leverages Exelis signal domain knowledge of GNSS
- > Patented Exelis Technology
- > Signal Sentry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



Assures safety, efficiency, and revenue

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



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

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

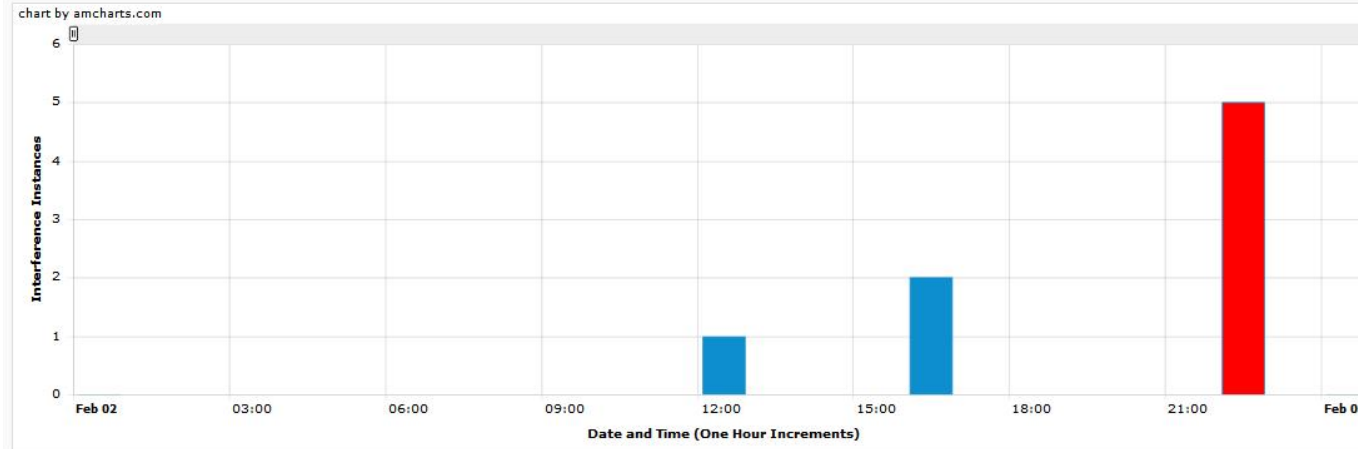


This document is not export controlled. Use or disclosure of this information is subject to the restrictions on the Title Page of this document.

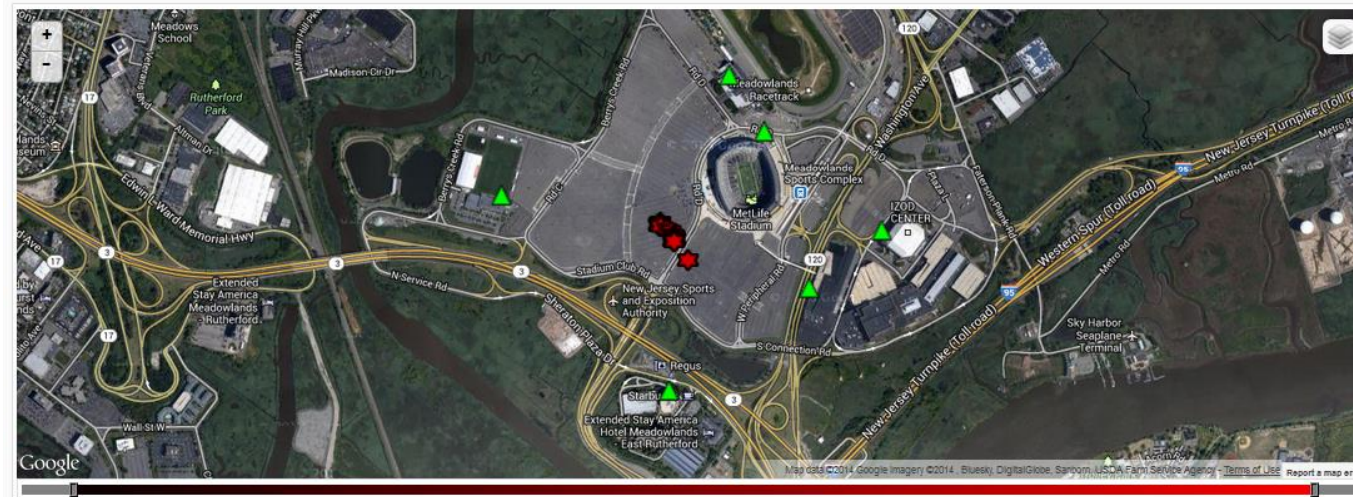
Interference Frequency – When & Where?

Interferer Frequency

Geolocated Instances of Interference Timeline (One Hour Increments) From Sunday, February 02, 2014 12:00:00 AM To Monday, February 03, 2014 12:00:00 AM



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.

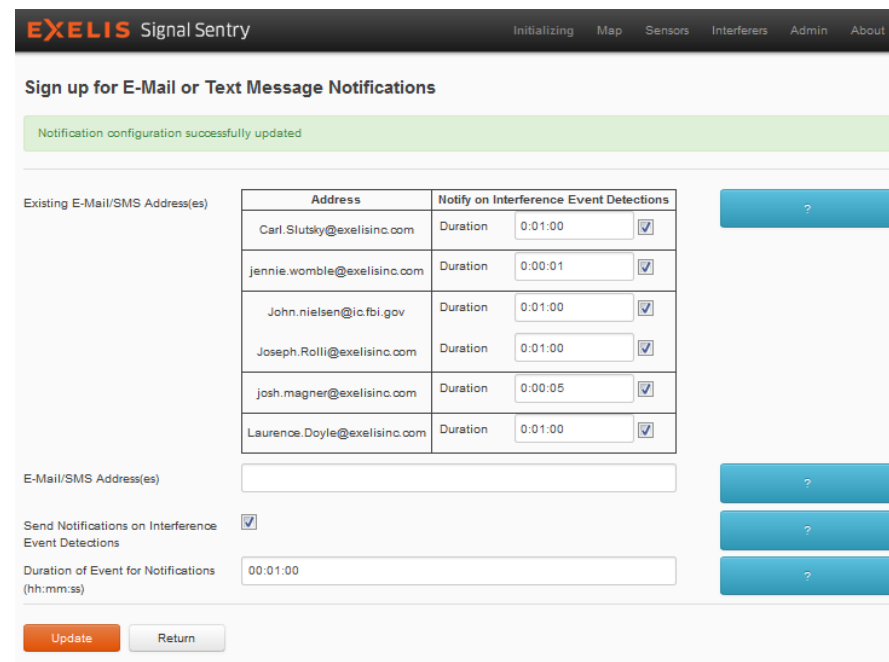
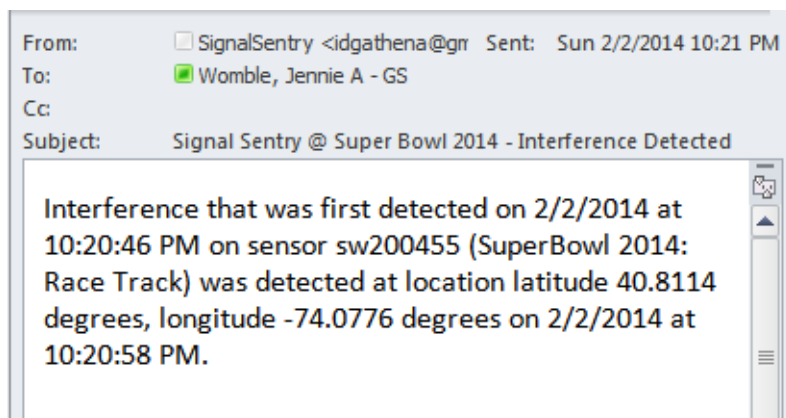


- Selecting histogram bar displays location of events on map below
- Can select more than one bar at a time

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

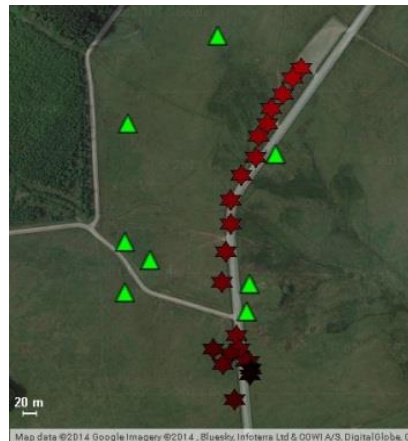
Alerts – Provides Real-time Actionable Intelligence

- Users can sign up for text or email alerts
- Alert sent when event has exceeded the user-defined duration
- Second alert sent once event has ended
- Alert signup is found under the Admin Menu



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

- 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
- Identified jammers in moving vehicles within a 10-meter accuracy



Jammer in car at 50 mph

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

- > Shipping Ports (Southampton UK)
 - > \$12.4B global maritime security expenditure 2011
- > Law Enforcement (Newark NJ)
 - > Global law enforcement equipment market to reach \$6.99B in 2015
- > Airports
 - > \$19.10B global airport security expenditure 2011
- > Security (Super Bowl)
 - > 2300+ municipalities are executing Safe City projects with price tags reaching \$B's (e.g. Dubai \$2.3B, Guangdong Province \$6B, etc.)



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

- > [Brochure](#) (A4 Available)
- > Presentation
- > [Position Paper](#) on the Threat
- > Infographics
 - [Importance of GPS](#), how it works and Exelis
 - [Signal Sentry 1000](#)
- > [Data Sheet](#)
- > [Video](#)



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

- > Most sectors of the economy rely on GPS
- > GPS jamming devices becoming cheaper and more accessible
- > Signal Sentry 1000 delivers actionable interference intelligence
 - Defends against disruption of guidance, traffic and asset control systems
 - Improves situational awareness
- > Detects and Locates GPS Jamming
- > Provides Actionable Intelligence

Signal Sentry 1000 – Assures safety, efficiency, and revenue



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