GPS Interference Detection & Mitigation

National GNSS Research Center Workshop

Daejeon, KOREA

08 April 2011

Jeffrey Auerbach
GNSS Policy Advisor
Office of Space and Advanced Technology
U.S. Department of State

Overview

- LightSquared and potential GPS Interference
- U.S. Spectrum Management Process
- Interference Detection and Mitigation
  - Planned “Patriot Watch” Program

Existing/Emerging Global Threats

GPS and GSM Jammer

U.K. £150

1 Watt Jammer

Links between Criminal & Terrorist activity are indisputable

GPS Navigation Devices Can Be Duped

Just like flat-screen televisions, cell phones and computers, global positioning system (GPS) technology is becoming something people can't imagine living without. So if such a ubiquitous system were to come under attack, would we be ready?

It's an uncomfortable question, but one that a group of Cornell researchers have considered with their research into "spoofing" GPS receivers.

GPS is a U.S. navigation system of more than 30 satellites circling Earth twice a day in specific orbits, transmitting signals to receivers on land, sea and in air to calculate their exact locations. "Spoofing," a not-quite-technical term first coined in the radar community, is the transmission of fake GPS signals that receivers accept as authentic ones.

Todd Humphreys, right, discusses with Paul Kintner, left, and Mark Psiaki how a GPS receiver can be "spoofed," based on the research work at Cornell. Robert Barker/University Photography

The Washington

Gunmen Used Technology as A Tactical Tool

Haste Could Make Waste

Obama Teams Are Scrutinizing

Coaxing!

Aug 08, FCC cites Colorado business for selling GPS jammers to counter GPS vehicle trackers

WA Post Aug 08

Police Turn to Secret Weapon: GPS Device

By Jack Hitt
Washington Post Staff Writer

Someone was stalking women in Fairfax County and Alexandria, grabbing them from behind and sometimes punching and molesting them before running away. After logging 11 cases in six months, police finally identified a suspect.

David Lee Foltz Jr., who had served 17 years in prison for rape, lived near the crime scenes. To figure out if Foltz was the assailant, police pulled out their secret weapon: They put a Global Positioning System device on Foltz's van, which allowed them to track his movements.

Police said they soon caught Foltz dragging a woman into a wooded area in Falls Church. After his arrest on Feb. 6, the string of assaults suddenly stopped. The break in the case relied largely on a crime-fighting tool they would rather not discuss.

"We don't really want to give any info on how we use it as an investigative tool to help the bad guys," said Officer Shelley Buckwalter, a Fairfax police spokeswoman. "It is an investigative tool for us, and it is a very new investigative tool."

Across the country, police are using GPS devices to snare thieves, drug dealers, sexual predators and killers, often without a warrant or court order. Privacy advocates said tracking suspects electronically ...

See GPS DEVICES, A12, Col. 1

LightSquared & GPS

- Plans to provide a nationwide wireless broadband network integrated with satellite coverage
  - Combine existing mobile satellite communications services with a ground-based wireless communications network that uses the same L-band radio spectrum as the satellites
  - Network will transmit signals in a radio band immediately adjacent to the GPS frequencies (1525-1559 MHz/1626.5-1660.5 MHz band)
  - Concern that ground-based transmissions may interfere with GPS signal
- 18 November 2010 - Request submitted to FCC for modification of its (ancillary terrestrial component) ATC authority
- 26 January 2011 - FCC Order & Authorization
  - Conditional approval to build out its ground-based wireless network
  - Requires addressing GPS concerns

LightSquared & GPS Interference

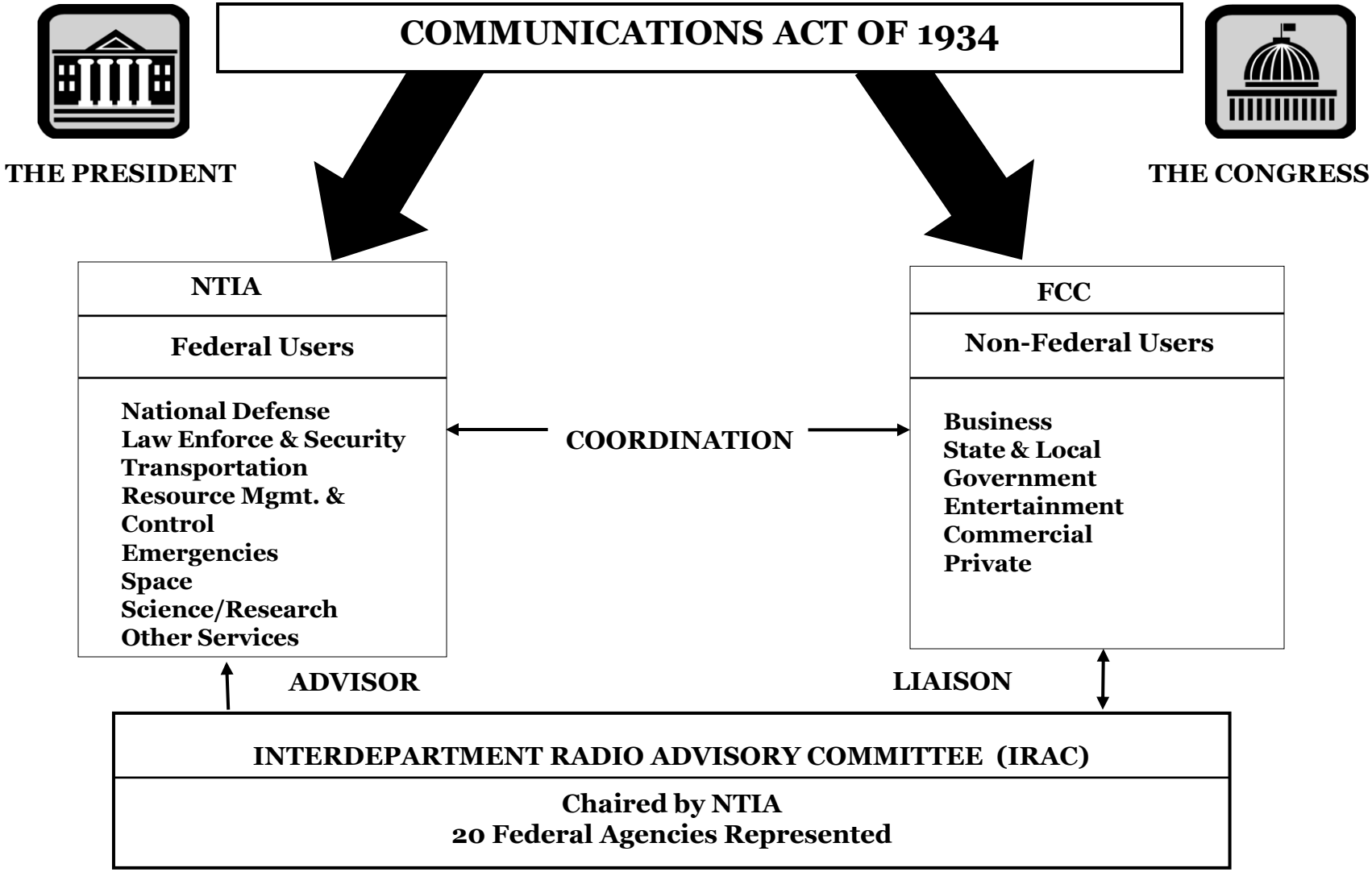
- FCC required that LightSquared create a working group with the GPS community to address interference concerns
  - Final report to be submitted by 15 June 2011
  - Process must be completed to the Commission's satisfaction before commencement of commercial service
- U.S. Government's National Space-Based PNT Systems Engineering Forum (NPEF) is conducting its own testing of the potential interference to GPS from the terrestrial network

www.pnt.gov/interference/lightsquared/

U.S. Domestic Spectrum Management Process

- In the United States, responsibility for spectrum management including **frequency allocations** is divided between Federal Government uses and other uses
- The National Telecommunications and Information Administration (**NTIA**) is responsible for Federal Government uses, while the Federal Communications Commission (**FCC**) is responsible for all other uses
- Where responsibilities overlap, the **FCC** and **NTIA** reach a consensus through coordination

National Spectrum Management



Regulations in the U.S.

- U.S. Federal statutes and regulations generally prohibit the manufacture, importation, sale, advertisement, or shipment of devices, such as **jammers,** that fail to comply with FCC regulations
- U.S. Federal Statutes – Communications Act
  - 47 U.S.C. § 301 Unlicensed (unauthorized) operation prohibited
  - 47 U.S.C. § 333 – Willful or malicious interference to authorized communications prohibited
  - 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

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 all applicable administrative, technical, labeling and identification requirements.
  - 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."

FCC Education Campaign

JAMMING CELL PHONES AND GPS EQUIPMENT IS AGAINST THE LAW!

In recent years, the number of websites offering "cell jammers" or similar devices designed to block communications and create a "quiet zone" in vehicles, schools, theaters, restaurants, and other places has increased substantially. While these devices are marketed under different names, such as signal blockers, GPS jammers, or text stoppers, they have the same purpose. We remind and warn consumers that it is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi. Despite some marketers' claims, consumers cannot legally use jammers within the United States, nor can retailers lawfully sell them.

Why are jammers prohibited? Use of jamming devices can place you or other people in danger. For instance, jammers can prevent 9-1-1 and other emergency calls from getting through or interfere with law enforcement communications (ambulance, fire, police, etc). In order to protect the public and ensure access to emergency and other communications services, without interference, the FCC strictly prohibits the use, marketing, manufacture, and sale of jammers.

What happens if you use a jammer? Operation of a jammer in the United States is illegal and may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.

Want to file a complaint or need more information? To file a complaint alerting the FCC's Enforcement Bureau to illegal cell, GPS, or other jamming devices, please visit www.fcc.gov/complaints or call 1-888-CALL-FCC. Additional information about jammer enforcement is available at www.fcc.gov/eb/jammerenforcement or by emailing the Enforcement Bureau at jammerinfo@fcc.gov.

Issued by the Enforcement Bureau of the Federal Communications Commission

www.fcc.gov/eb/jammerenforcement/

National Space Policy

Radiofrequency Spectrum and Interference Protection

- The United States Government shall:
  - Protect global access to the radiofrequency spectrum required to support the use of space by the United States Government, its allies, and U.S. commercial users
  - Address requirements for radiofrequency spectrum in the acquisition of space capabilities
  - Ensure necessary regulatory frameworks remain in place over the lifetime of a system;
  - Identify impacts to government space systems prior to reallocating spectrum
  - Enhance capabilities and techniques, in cooperation with civil, commercial, and foreign partners, to identify, locate, and attribute sources of radio frequency interference
  - Take necessary measures to sustain the radiofrequency environment in which critical U.S. space systems operate
- Invest in domestic capabilities and support international activities to detect, mitigate, and increase resiliency to harmful interference to GPS

Critical Infrastructure and Key Resources (CIKR) Sectors


Agriculture and Food


Banking and Finance


Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy


Government Facilities


Healthcare and Public Health


Information Technology


National Monuments and Icons


Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems


Water

U.S. Interference Detection & Mitigation Initiatives

- DATA: Collect, analyze, store, & disseminate interference incidents from all reporting sources
- TOOLS: Coordinate U.S. domestic capabilities to identify, analyze, locate, attribute, & mitigate sources of interference to the GPS & its augmentations
- ACTION: Develop & maintain capabilities, procedures & techniques, & routinely exercise civil contingency responses to ensure continuity of operations in the event that access to GPS signal is disrupted or denied

Planned U.S. "Patriot Watch" System

- System-of-Systems, open architecture, multi-phased approach to provide near real-time situational awareness of GPS in order to detect EMI & suspect purposeful interference to protect the Nations 18 CIKR Sectors
  - Designed with government and commercial hardware/software
  - Persistent monitoring for situational awareness
  - Timely response to anomalies
  - Sensor placement based on PNT CIKR Criticality
  - Remains operational when GPS systems is "stressed"

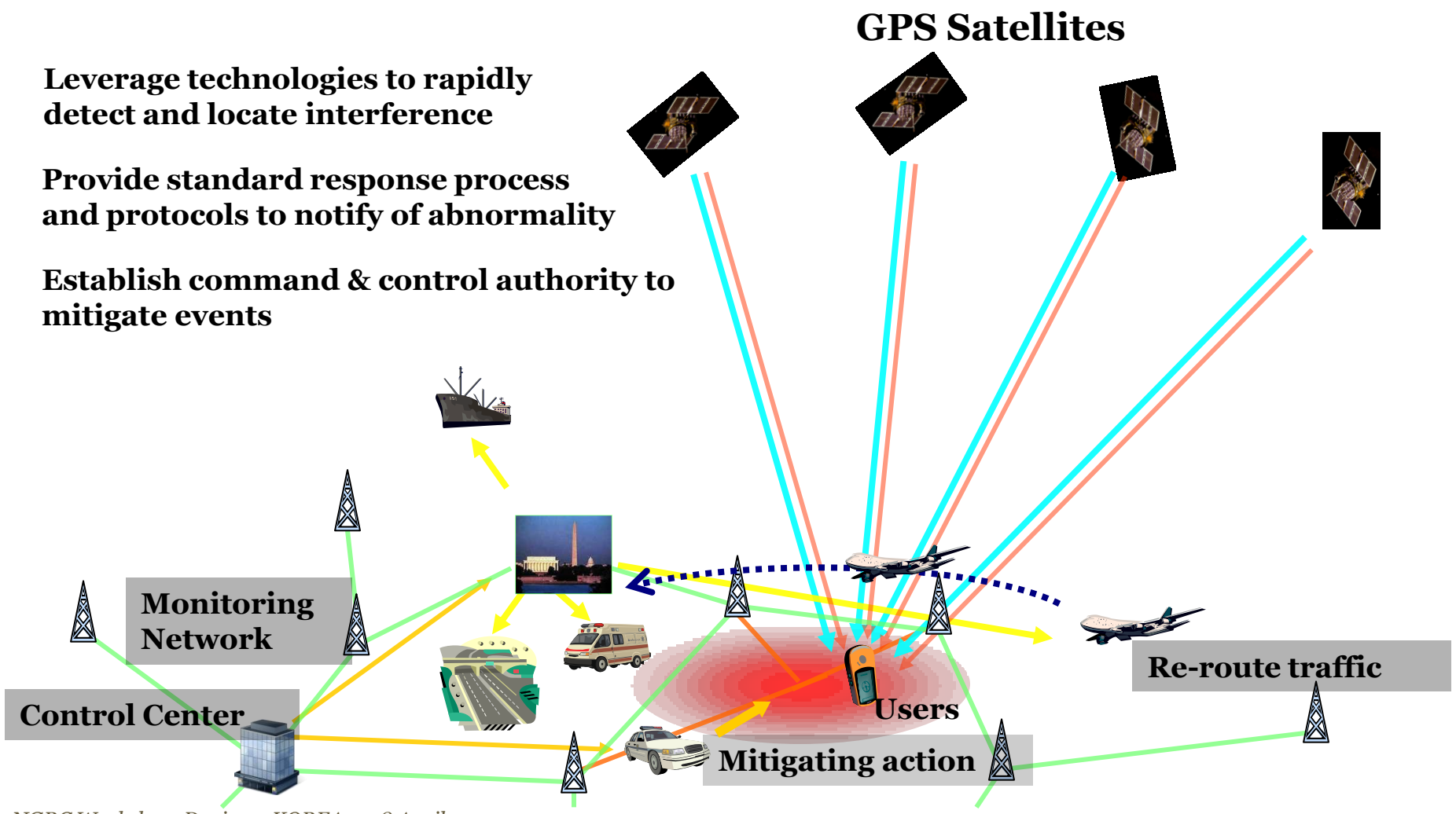
"Patriot Watch" Concept

National capability to detect & mitigate GPS interference in the U.S.

Leverage technologies to rapidly detect and locate interference

Provide standard response process and protocols to notify of abnormality

Establish command & control authority to mitigate events



Summary

- Concerns over potential GPS interference from LightSquared proposal are being studied
- Civil infrastructure use of GPS drives requirement to build a **national IDM capability**
- **"Patriot Watch"** will provide situational awareness for Homeland Security and Homeland Defense
- Collaboration has been and continues to be a key element on building a successful system