Department of Transportation
Office of the Secretary
Office of the Assistant Secretary for Research and Technology (OST-R)

Information Security and Privacy Advisory Board

March 4, 2021

Reliable Navigation and Timing is Critical for Transportation

Aviation – NextGen

- Reliable and accurate positioning worldwide
- Reduced delays
- More fuel-efficient routes
- Increased system capacity with enhanced safety

Intelligent Transportation Systems

- Enable crash prevention among vehicles and between vehicles and infrastructure

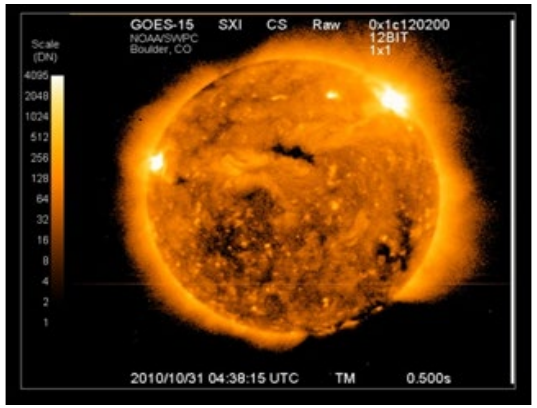
Rail – Positive Train Control

- Reduced probability of collisions
- Increased efficiency and capacity

Maritime

GPS/GNSS Challenged Environments

Ionospheric Disturbances



High Accuracy with Integrity

Timely Notification of Misleading Information

Underground/Indoors

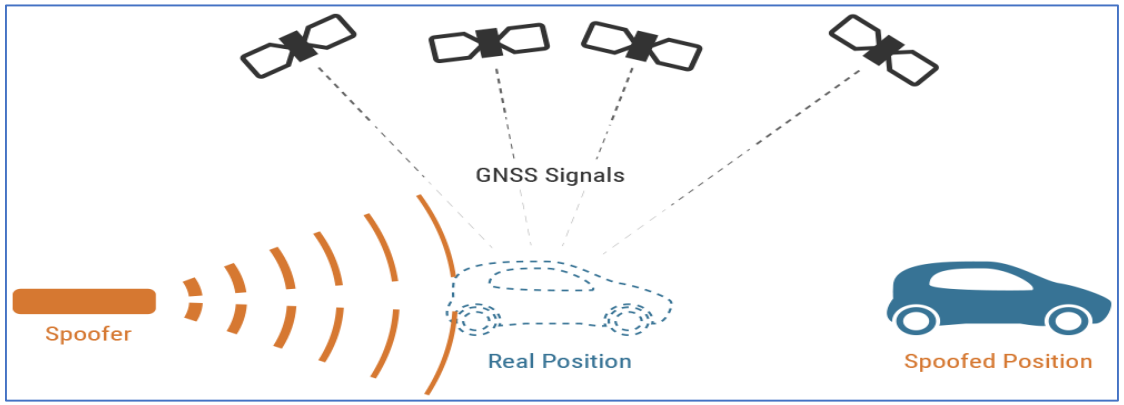
Urban Canyons

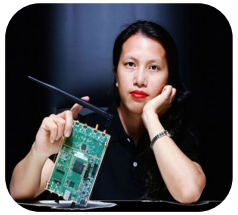
Inaccurate/Out-of-Date Maps

Existing GPS/Global Navigation Satellite System Threats

- Jamming is intentionally produced RF waveforms that have the same effect as interference; the only difference is the intent to degrade or deny a target receiver's operation.

- Spoofing can deny, degrade, disrupt, or deceive a receiver's operation and can have a range of effects from incorrect outputs of PNT to receiver malfunction. The onset of these effects can be instantaneous or delayed and it is possible for effects to continue even after the spoofing has ended. Ref. DHS Report "*Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*"





2018 National Science Foundation grant to University of Virginia published: ROAD TO NOWHERE — $225 GPS Spoofer can send SATNAV-guided vehicles into oncoming traffic.

Executive Order 13905 February 12, 2020

Purpose: Foster responsible use of PNT services by critical infrastructure owners and operators to strengthen national resilience

Policy: Ensure disruption or manipulation of PNT services does not undermine reliability or efficiency of critical infrastructure

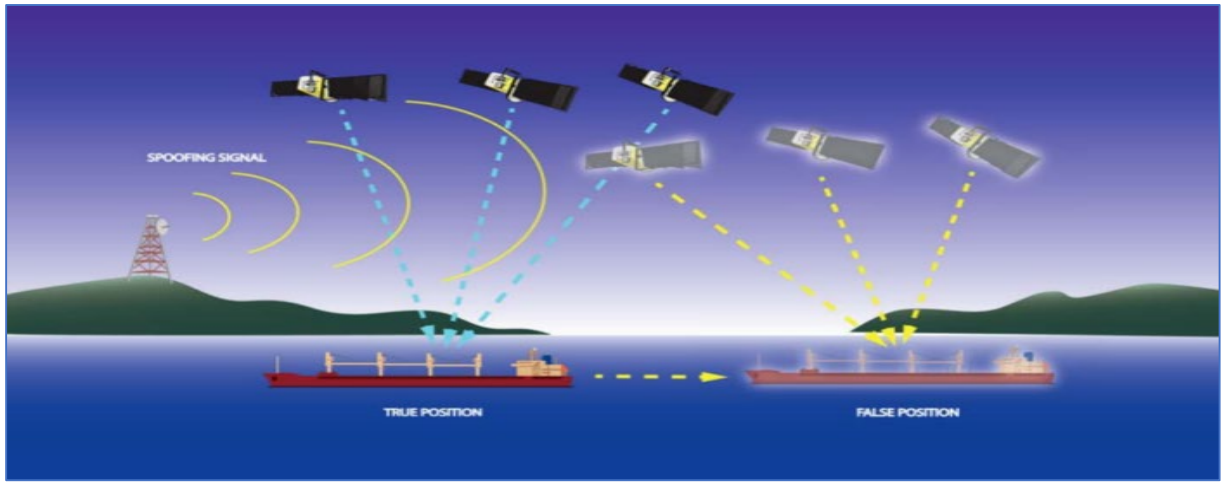
- Raise awareness of the extent to which critical infrastructure depends on PNT services
- Ensure critical infrastructure can withstand disruption or manipulation of PNT services
- Engage public and private sectors to promote responsible use of PNT services

Key Actions:

- PNT Profile Development – NISTIR 8323
- National R&D Plan on PNT Resilience
- Pilot Programs / Vulnerability Assessment / Testing
- GNSS Independent Source of UTC

DOT Pilot Program Overview

- Focus on addressing GPS jamming and spoofing impacting maritime vessels:
  - Conduct stakeholder engagement
  - Evaluate Complementary PNT technologies suitable for the maritime environment
  - Develop a jamming and spoofing detection capability



- Results will provide insights to support the development of PNT profiles for maritime applications, as well as to inform additional PNT R&D
- Results and lessons learned may benefit PNT resiliency for other modes of transportation (aviation, rail, vehicles, and pipeline)

GPS Jamming and Spoofing in the Maritime Environment

- DOT public workshop held December 3, 2020
- 426 Registrants
- USG Briefers: NSC, OST-R, MARAD, USCG, Volpe Center
- Industry Briefers: Maersk, APL Maritime, RNT Foundation
  - Operational experience/impacts from GPS jamming and spoofing

Presentations available at:

https://www.transportation.gov/pnt/agenda-virtual-workshop-gps-jamming-and-spoofing-maritime-environment

GPS Backup/Complementary PNT Demonstration

- Awarded 11 PNT technology vendor demonstration contracts on rapid acquisition purchase orders through OST-R/Volpe Center
  - Technologies included: Terrestrial RF, Low Earth Orbit, Fiber Optic, and Map Match
- Executed three field campaigns, technology demonstration, and analysis and assessment of data
- Report to Congress submitted on January 15, 2021 (along with NTRSA Report)

PNT Technology Vendor Participation

Vendor	Technology	Site	Timing Scenarios					Positioning Scenarios			
			Demo Site	72-Hr Bench Static Timing	Static Outdoor Timing	Static Indoor Timing	Static Basement Timing	Reference Station Offset (eLORAN Timing)	Dynamic Outdoor Positioning with Holds	Static Outdoor Positioning	Static Indoor Positioning	Airborne 3D Positioning
Echo Ridge LLC	LEO commercial S-band (2483.5 - 2500 MHz)	LaRC					N/A		X		
Hellen Systems, LLC	eLORAN terrestrial RF (90-110 kHz)	JBCC	X			X	X				
NextNav LLC	UHF terrestrial RF (920 - 928 MHz)	LaRC	X	X	X	X	N/A	X	X	X	X
OPNT B.V.	fiber optic time service (white rabbit PTP)	LaRC	X				N/A				
PhasorLab Inc.	802.11 terrestrial RF (2.4 GHz)	JBCC	X	X	X		N/A	X	X		X
Satelles, Inc.	LEO commercial L-band (1616 - 1626.5 MHz)	JBCC	X	X	X	X	N/A		X		
Serco Inc.	R-mode terrestrial RF (283.5 - 325 KHz)	JBCC					N/A	X	X		
Seven Solutions S.L.	fiber optic time transfer (white rabbit PTP)	LaRC	X				N/A				
Skyhook Wireless, Inc.	802.11 terrestrial RF (900 MHz, 2.4 & 5 GHz)	LaRC					N/A	X	X	X	X
TRX Systems, Inc.	UWB & IMU map matching (3.1 - 5 GHz)	LaRC					N/A	X*	X	X	
UrsaNav Inc.	eLORAN terrestrial RF (90 - 110 kHz)	JBCC	X		X	X	X				
GPS (SPS PS)	MEO government L-band (1575, 1227, 1176 MHz)	All	X	X			X	X	X		X

*static holds only

Key: N/A Technology incompatible with scenario definition

Observations from the FY18 NDAA PNT Demonstration

- FY'18 NDAA GPS Backup and Complementary PNT Demonstration results indicate there are suitable and mature private-sector PNT technologies that have the potential to meet a diversity of application-specific needs.

- The FY'18 NDAA demonstration was designed to showcase technologies in the "best light" possible
  - Complementary PNT technologies were not stress-tested.

- The transportation sector has some of the most stringent PNT performance requirements in terms of accuracy, integrity, availability, and reliability.
  - Not all safety-critical transportation requirements may be met by market-based business models for PNT technologies.

- Private-sector Complementary PNT technologies do not currently have the level of open specifications and standards that have made GPS such a critical and widely adopted service.
  - A similar level of standards, resiliency and vulnerability testing, and performance monitoring must be developed for these technologies.

Complementary PNT: Recommended Next Steps

1. Safety-critical PNT requirements and standards development for transportation services

2. PNT vulnerability and performance testing framework for demonstrated and suitable complementary technologies
   - Procedures, facilities, and platforms for testing PNT performance and resilience to threats
   - Certification protocols for safety-critical PNT functions

3. PNT performance monitoring capabilities to ensure operational PNT services provide resilience and achieve safety-critical standards for transportation and critical infrastructure applications

DOT Focus on PNT for Highly Automated Systems

PNT for Automated Vehicles (AV): ITS Joint Program Office

- AV use cases / scenarios
- Determine PNT requirements for AV operations
- Assess GNSS and other candidate sensor technologies
- Analyze PNT performance of individual sensors
- Determine navigation performance enhancements achieved by sensor fusion

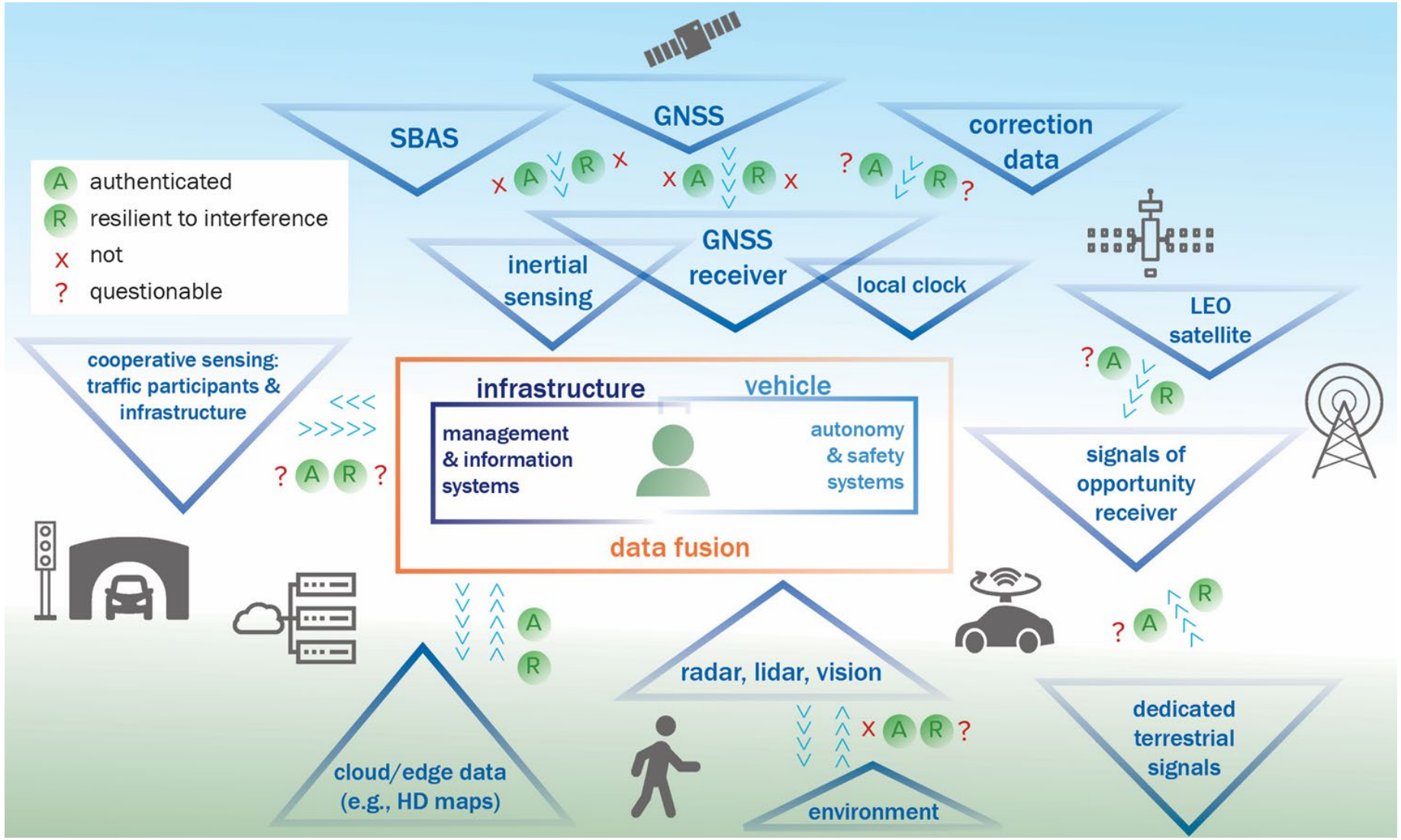
DOT University Transportation Center: Highly Automated Transportation System Research

- Vulnerability cataloging and test threat vector development
- Resiliency testing
- Standards, Guidelines, and Best-practices for cyber resiliency

OST-R Highly Automated System Safety Center of Excellence

- Resilient PNT Services for Highly Automated Safety Systems
- Focus on NIST PNT Profile

University Transportation Center Vision for PNT Resiliency



Summary

- **Protect**
  - Ensure performance monitoring of space-based civil PNT services
  - Facilitate international coordination for development of monitoring standards
  - Implement interference monitoring capabilities to identify, locate, and attribute PNT threats
  - Prevention of harmful interference
- **Toughen**
  - Authenticate signals and harden user equipment (receiver/antenna/algorithms)
- **Augment**
  - Utilize GPS augmentation and Complementary PNT services