National Space-Based PNT Advisory Board Update

Dr. Bradford Parkinson

Vice Chair PNTAB

Original Program Director and Chief Architect of GPS
Founder of GPS Research Center at Stanford University

The Honorable John Stenbit

Chair PNTAB

Member of the Defense Science Board, the National Security Agency Advisory Board, the STRATCOM Advisory Board, and the National Reconnaissance Office Advisory Group.

Former Assistant Secretary of Defense for Command, Control, Communications, and former Department of Defense (DoD) Chief Information Officer

Introduction PNTAB

- Primary PNTAB Objective (ongoing - the major focus)
  - Assured ***PNT*** for all Users
- Current Assessment
  - No current or foreseeable alternative to GNSS
  - **Selected** Addressable Threats
    - Authorized ***repurposing of adjacent*** RF bands (FCC authorizatio
    - ***Deliberate Jamming*** (e.g. inexpensive small jammers)
    - *Deliberate Spoofing* – misleading signals causing false GPS measurements

Today's Review

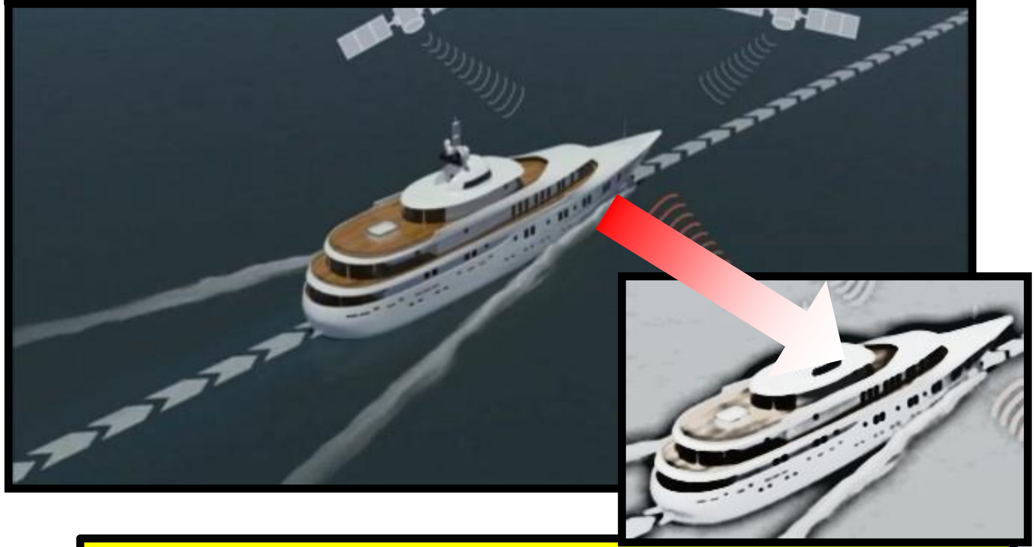
- PNTAB advocated Strategy - the ***PTA Program***
  - ***P***rotect the radio spectrum + identify + prosecute interferers
  - ***T***oughen GPS receivers against natural and human interference - *(Spoofing and Jamming)*
  - ***A***ugment with additional PNT sources and Techniques

Deliberate Spoofing is a Real Threat

Many examples of Spoofing recently, Real and Possible:

- Academic Demonstrations
- Possible Incidents for Military
- Will focus on "Civilian" Receivers
- Military has additional anti-spoofing techniques

"Professor fools $80M superyacht's GPS receiver on the high seas"



Humphreys conducted the test in the Ionian Sea in late June 2013 and early July 2013 with the full consent of the "White Rose of Drachs" yacht captain.

- Outline:
  - – What is Spoofing?
  - – How can it be prevented?
  - – What actions might USG take?

Spoofing Definition and General Techniques

Spoofing:

- ***Deliberately creating False GNSS signals that lead to misleading Position, Time or Velocity***

Note: Not considering *inadvertent satellite errors* –an integrity problem, albeit has some of the same solutions

- ***A Few Examples*** *of Deliberate Spoofing* ***Techniques***

Technique 1. ***Create*** fictitious signals & broadcast to user

- Presumably Hazardous and Misleading Information ("HMI")
- Requires Knowledge of Signal Sequences
- Requires time synchronization

Technique 2. ***Rebroadcast*** GPS signals with >> Power

Arrives at user with a delay – nanosecs to 10s of microseconds

Technique 3. Combination of 1 and 2.

Spoofing Defense levels

- ***Spoofing Defense Levels***
  1. Detect and:
     A. Do not use spoofed signal - *May totally deny use of GNSS*
     B. Do not use ***plus operate through***
  2. Substantial Immunity – not detected because no harmful effect

Bottom Line Up Front – Don’t be Gullible:

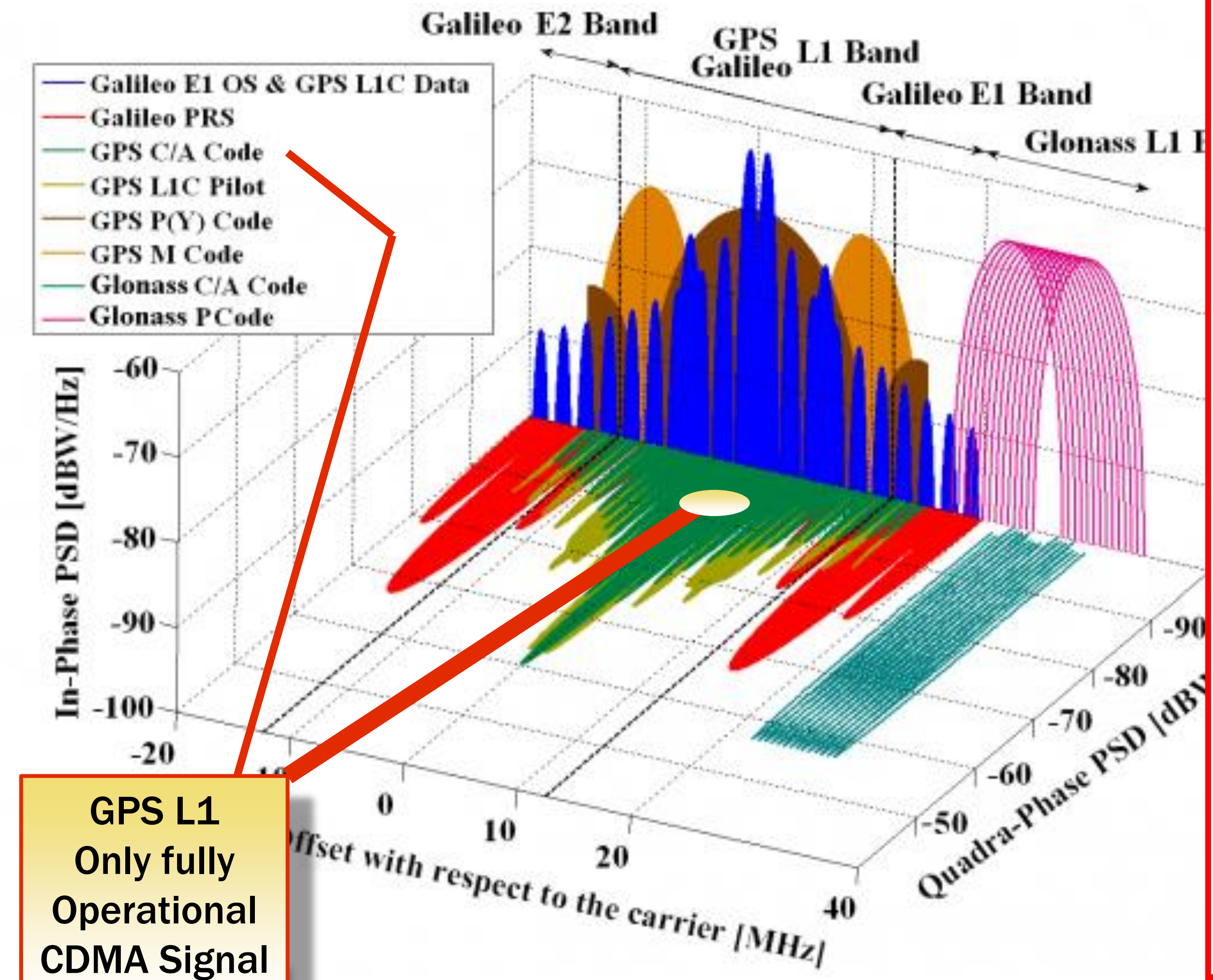
“Competent” (i.e. skeptical) PNT receivers should be immune to virtually any type of spoofing attack

Spoofing Defense Techniques

- “Competent” (Skeptical) receivers should detect spoofing
  - at a minimum, cleanly stop providing misleading outputs
  - Consistency checking (“crosschecking” – a self-integrity monitor) Use of
    - all GPS satellites in View
    - other Validated GNSS
    - Augmentations
  - Signal inspection
- Most Receivers should be able to “Operate through

Well-known defenses are generally not being incorporated

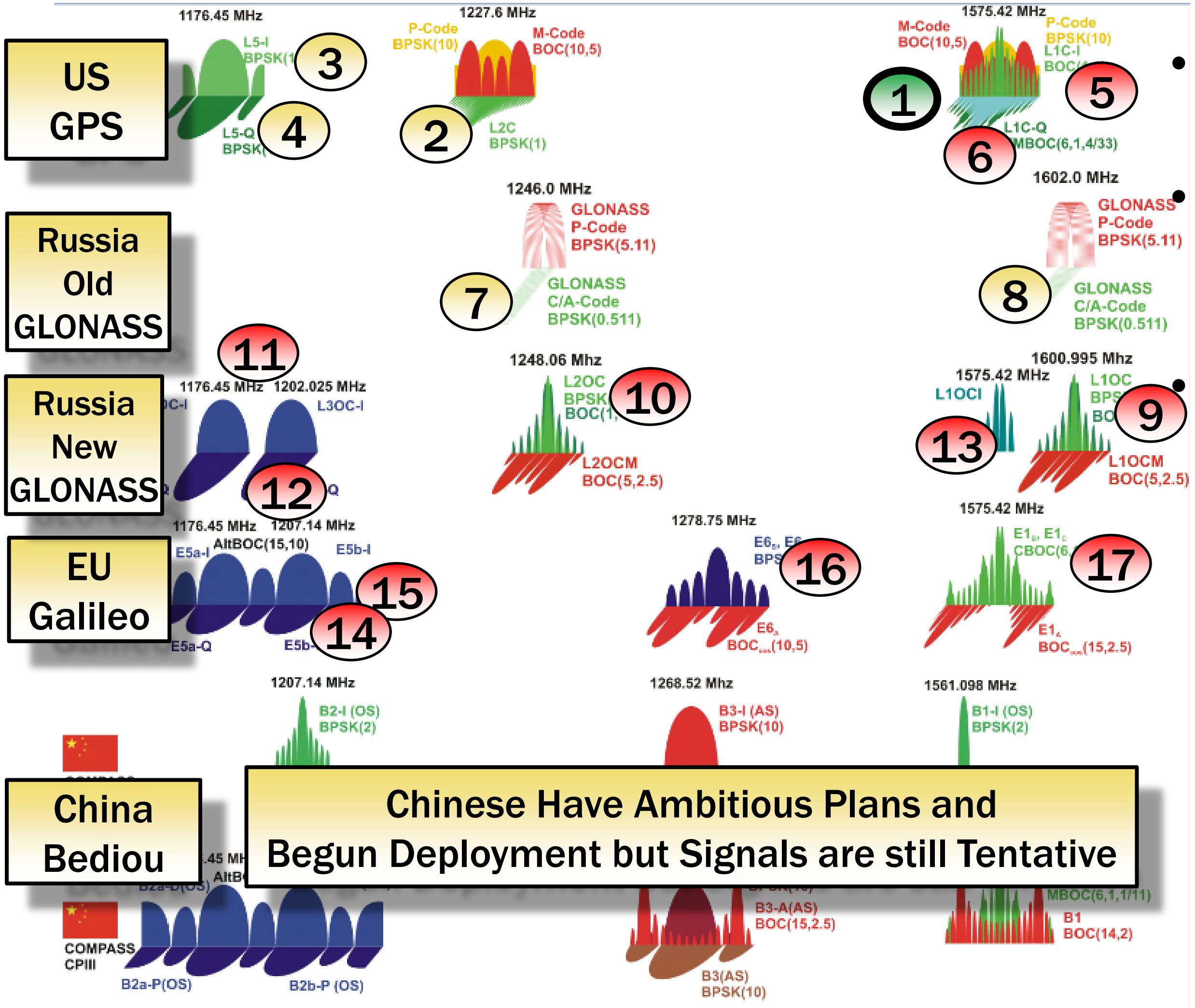
GNSS Signals in the Upper Band



GPS L1
Only fully
Operational
CDMA Signal
today

- Only one of three GNSS Frequency Bands is shown
- Many Integrity checks will soon be available
- But must be incorporated into PNT Receivers

More Opportunities: Current and Planned *Civil* GNSS Signals



Chinese Have Ambitious Plans and Begun Deployment but Signals are still Tentative

Green Civil (Fully or Partially Deployed)

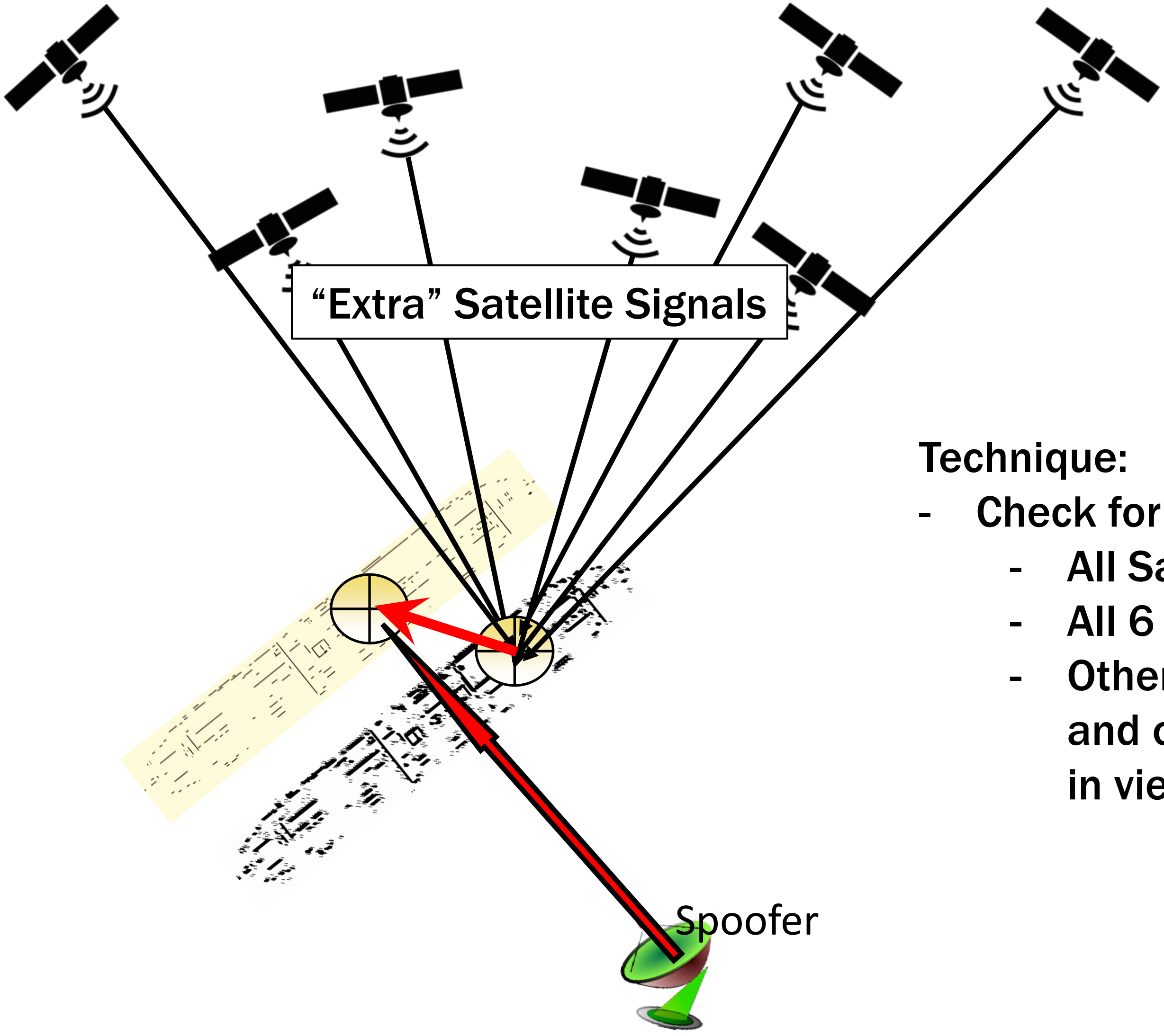
Blue Civil (Planned or experimental)

Red -Restricted

- Only Fully Operational CDMA signal is GPS L1 C/A 1
- Partially operational are GPS L2C and L5 2 3 4 GLONASS L1 & L2 7 8
- Under Development 5 6 & 9 to 17

- **The Message:**
- Only *one anti-spoof* crosscheck signal is used today by most “skeptical’ receivers
- At least 5 more are partially available
- Within 7 years should have over 17 signals on about 30 satellites in View for Anti-Spoofing

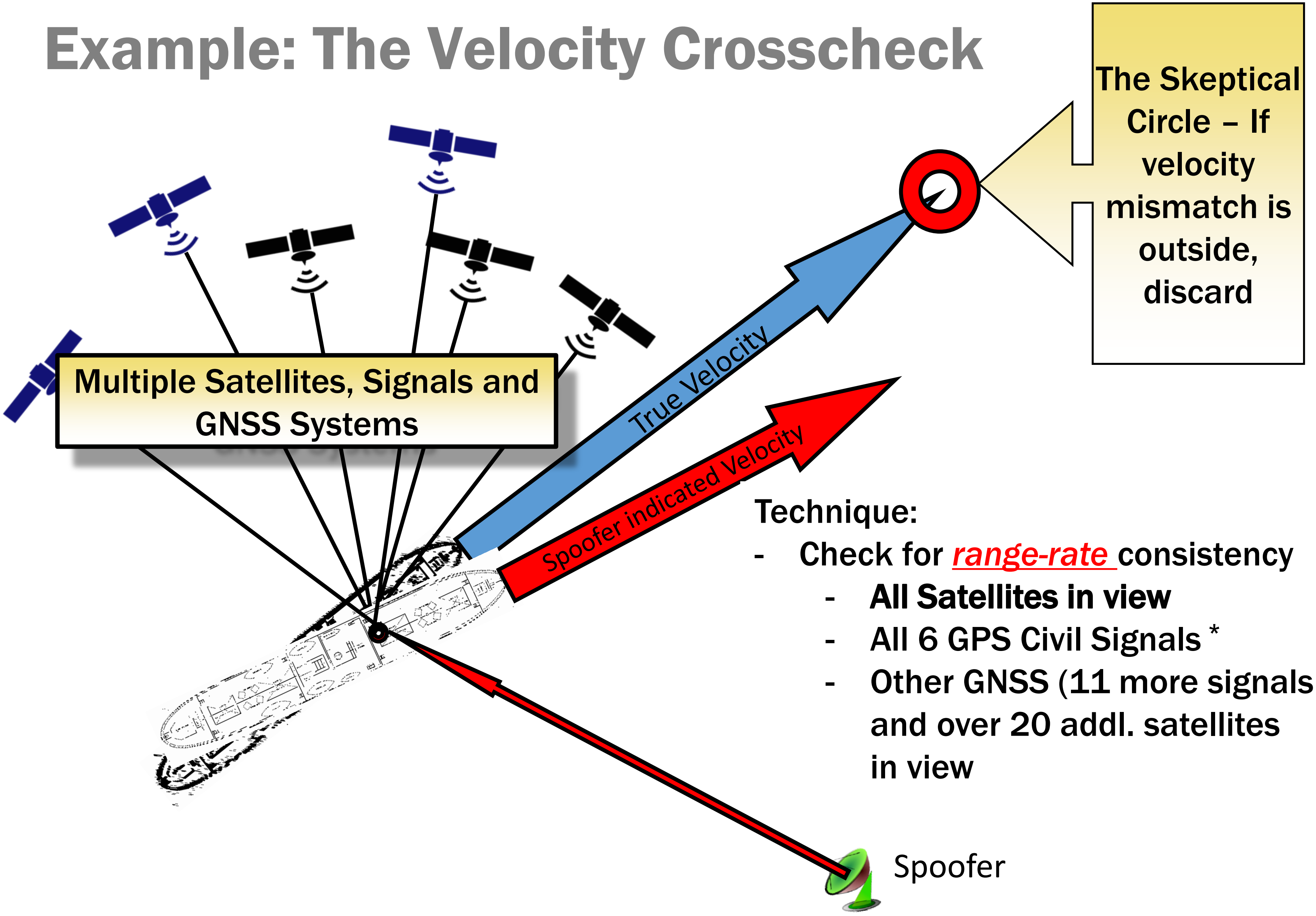
Example: The Positioning Crosscheck



Technique:

- Check for ***ranging*** consistency
  - All Satellites in view
  - All 6 GPS Civil Signals *
  - Other GNSS (11 more signals and over 20 addl. satellites in view)

Example: The Velocity Crosscheck



Multiple Satellites, Signals and GNSS Systems

The Skeptical Circle – If velocity mismatch is outside, discard

Technique:

- Check for *range-rate* consistency
  - **All Satellites in view**
  - All 6 GPS Civil Signals *
  - Other GNSS (11 more signals and over 20 addl. satellites in view

Spoofing Detection Techniques

Just Illustrated

- Inter-System Crosschecks (GPS will soon have 6 Civil signals)
  - GPS - 9 to 11 Satellites in view – 5 to 7 are "redundant"
    - Traditionally Position checks
    - GPS velocity - more precise than 1/10th of a mile per hour
    - Satellite Time (10s of nanosecond comparisons)
- Intra-GNSS Cross Checks (Use of Validated Galileo etc)

Additional Methods

- Antennas that attenuate spoofing and interference
  - Amplify Valid Signal
  - Attenuate Spoofing input
- RF environment monitoring: local, regional, national
  - Input Power above normal
- External Detection and Notification – FAA's WAAS?
- Other System Crosschecks
  - Inertial Navigation Components
  - Other RF Systems – ***eLoran or FAA's DME***
  - Eyeballs/ Magnetic Compass etc.

Barriers to Crosschecks for Spoofer Prevention

(most cost-effective technique)

- Not implemented in many (Naïve) receivers today
  - Can be virtually free to users
  - Threat apparently not appreciated by manufacturers
- New GPS wide band signals very useful (e.g. L1C)
  - Expanding from 1 to 6 signals at 3 Frequencies
  - Greater exposure to repurposing adjacent bands
- Other satellite Systems (GNSS – Galileo, GLONASS et al) ***3 addl freq. - but <u>not authorized in US</u>***
  - Europeans will have full use of 3 systems, 6 frequencies, and 17 signals
  - ***<u>May be an FCC repurposing challenge</u>***
  - Integrity should be verified by FAA through WAAS

Our Message: Spoofing Vulnerability Must Be Reduced (And Techniques are well known)

- Need to develop and field "competent" receivers
  - Some of the techniques are nearly "free" for recurring cost
- Use and crosscheck multiple signals
  - Use existing second and third GPS frequencies (6 signals on the way!):
    - GPS L2C (19 satellites operating) and L5 (12 satellites operating)
  - Signals from other satnav systems Up to 17 in
    - Galileo should be particularly useful, but should to be "Integrity Monitored"
    - *Not currently authorized*
  - Other RF signals
    - FAA use of DME
- Field more selective antennas where needed
  - Very strong detection, and "operate through" technique

Recommendations (Reference PNTAB Letter Last Year to Sctys. Work and Mendez)

- *(Previous)* **Develop a Formal National Threat Model for PNT Applications in Critical Infrastructure**
  - **Should include updates on spoofing threats**
- **?? Establish a framework for using Foreign GNSS *with Integrity Validation*** **case by case – Galileo first?**
  - **General Permission to broadcast from space and receive**
  - **Include all-GNSS monitoring as part of FAA's WAAS/ Aviation infrastructure**
- *(Previous)* **Establish a Nationwide CONUS Back-Up to GPS with Existing Infrastructure (e.g. eLoran)**
  - ***Cannot achieve GPS level Accuracy* – but can "protect" 10s of meters in selected "differential" areas**
  - **Previously accepted by EXCOM**

Questions?

Current PNTAB Activity Focused on Three Major PNT Study Subjects

1. Assured Availability of ***PNT***

   – ***What actions*** can/should be ***taken to reduce vulnerability and ensure PNT Availability for all users***?

2. Affordability of ***PNT***

   – ***What actions*** can/should be ***taken to ensure PNT is Affordable for USG ?*** **e.g. satellites, jam resistant techniques…]**

3. Economic Value of ***PNT***

   – ***What is the World and the US Economic Value of GPS?***
   [And Impact in the event of Spectrum Denial]

PNTAB Recommendations

(Letter of 29 August to Sctys. Work and Mendez)

1) **Formally Designate GPS as a Critical Infrastructure Sector for the United States**

Virtually every Department of Homeland Security (DHS)-designated critical infrastructure sector is dependent on access to GPS for positioning, timing, or both. Specifically, these PNT services are pervasive elements in 14 of 16 critical U.S. sectors. Preliminary economic studies show a *direct* value of GPS equipment manufacturing of over $30B a year, which may triple to over $90B when also including the *indirect* benefits facilitated by the use of GPS. These impacts, however, are not yet fully understood nor appreciated by the critical infrastructure sectors, thus relegating GPS to a “stealth utility” status, lacking appropriate protections. Serious potential threats to GPS users range from changes in spectrum regulations, to intentional interference, cyber-attacks, spoofing, and even natural atmospheric disturbances. Such threats are credible and rapidly growing. It is therefore essential that resources and attention be focused on addressing such vulnerabilities. In order to achieve this goal, the PNTAB recommends that the DHS advocate and the President designate GPS as a *separate sector of critical infrastructure* and provide national leadership to counter these threats to our economy and security.

2) **Develop a Formal National Threat Model for PNT Applications in Critical Infrastructure**

The Department of Defense (DoD) routinely develops and updates threat models to GPS defense capabilities, and also prioritizes countermeasures to these threats. However, public safety GPS stakeholders, and other critical infrastructure sectors, do not have a validated threat model. We have studied this in some detail and strongly believe that there is a potential for serious national economic and public safety disruption. The PNTAB therefore proposes that the PNT National Coordination Office (NCO) be tasked and funded to lead the development of a detailed, PNT National Threat Model (PNT NTM) for GPS. This study should include all classes of threats, the probabilities and economic impacts, and outline potential countermeasures. The PNT NTM study should be developed in cooperation with *all* appropriately cleared civil GPS stakeholders, in particular GPS equipment manufacturers and PNT service providers. We believe the PNT NTM will enable federal departments and agencies, state and local governments, and commercial service providers to better understand and prioritize resource allocation for mitigation strategies.

3) **Prevent the Proliferation of Licensed Emitters in GPS Frequency Bands**

Recent regulatory proposals by the European Conference of Postal and Telecommunications Administrations (CEPT) would license certain terrestrial transmitters, or “pseudolites,” to operate in the primary GPS band (also known as GPS L1). This frequency band is designated as a Radionavigation Satellite Service (RNSS) and should be very carefully regulated. These transmitters pose a significant interference threat to GPS and other Global Navigation Satellite Systems (GNSS), including Europe’s emerging Galileo system. Therefore, the PNT AB recommends that the PNT EXCOM strongly oppose such licenses and that the U.S. Department of State urgently engage the European Signatories under a demarche pursuant to the terms of the 2004 U.S.-E.U. GPS-Galileo Agreement. The U.S. and the European Union should work cooperatively with the European Commission and CEPT, to prevent the authorization and proliferation of harmful devices in GNSS frequency bands.

4) **Establish a Nationwide CONUS Back-Up to GPS with Existing Infrastructure (eLoran)**

In 2006, an Independent Assessment Team (IAT), commissioned by DOT, unanimously recommended: “*Retain eLoran (enhanced Loran) as a primary backup for critical GPS applications.*” After studying the situation, thePNT AB unanimously concurred and made the same recommendation to the PNT EXCOM in 2007. The PNTEXCOM, with participation from all represented Federal departments, also unanimously concurred. Unfortunately, due to competing fiscal priorities, eLoran was cut from the budget in 2009 and its existing infrastructure is being dismantled. The PNT AB believes that existing Loran sites and antennae could provide an affordable path to a National GPS back-up system, and restated its recommendation at the last PNT EXCOM meeting held on March 14, 2014. We believe that the deployment of a national PNT back-up is now even more urgent due to the rapidly evolving threats to GPS-based PNT services. The PNT AB therefore reaffirms its previous recommendation and requests urgent action to preclude further dismantling of existing infrastructure that could be used as a GPS back-up to prevent disruptions to the U.S. economy, public safety, and security.

eLoran Previously Recommended by PNT EXCOM

- **Conclusions - (DOT IRB Dec 2006)**
  - Reasonable assurance of national PNT availability is prudent & responsible policy
    - For critical safety of life & economic security applications
    - And for all other “quality of life” applications
  - eLoran is cost effective backup – to protect & extend GPS – for identified critical (other GPS-based) applications
    - Interoperable & independent
    - Different physical limitations & failure modes
    - Seamless operations & *GPS threat deterrent*
  - Given US Government support, anticipate users will equip with eLoran as the backup of choice
    - International community also looking for US leadership
- **Recommendation**

Summary of Results from Independent Review Board
re: Loran - Convened by US/DOT (2006)

- Unanimous Recommendation – deploy eLoran
- DOT, DHS *and PNT EXCOM* supported the recommendation
- eLoran was a victim of Budget tightening
  dismantling existing LORAN stations was begun