PANEL 2 · CYBER-GEOSPATIAL CONVERGENCE

The digital border now runs through space–time.

Shielding digital borders from the Nordic–NATO frontline

Mikko Punnala, PhD (Space Economy) · Col (ret.)

Founder & CEO, Sharpnav · Finland
Founder & CEO, Space Air Technologies · Finland

1 MAY 2026

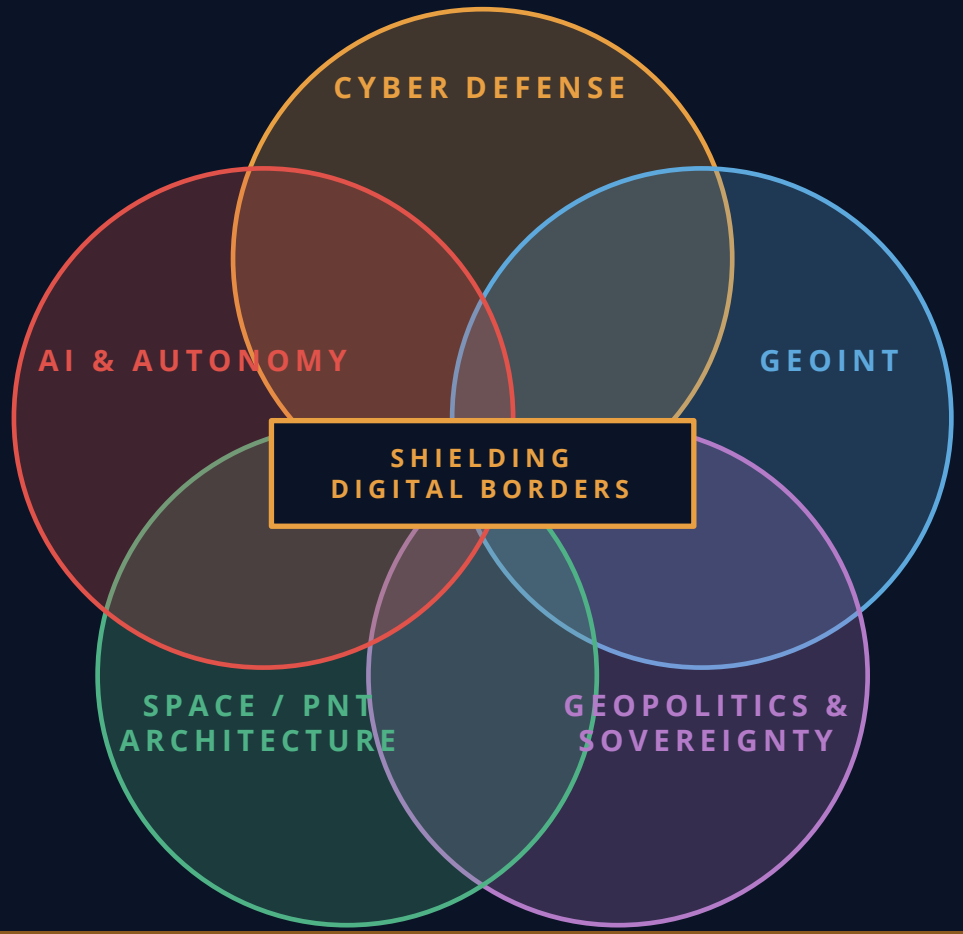
Hall E 104 · RAI Amsterdam

Chair: Prof. V.S. Subrahmanian

Co-panel: Dr. Anupam Tiwari

Five domains - One convergence

Shielding digital borders sits where five distinct domains intersect.



These five used to be separate disciplines. Today they are one architecture problem.

The frontline has already answered the question

Denial of signal integrity is now scaled, routine, and strategic

+220%

Increase in GPS signal-loss reports globally 2021–2024

Source: EASA / IATA

123,000

Flights disrupted in the Baltic–Nordic region Jan–Apr 2025

Source: Eurocontrol

7,500+

GPS interference events reported in 2023 (vs. ~1,500 in 2022)

Source: EASA

UKRAINE

PNT laboratory

- Russian EW (Pole-21, Tirada-2, Krasukha, Murmansk-BN) routinely denies GPS over the front.
- JDAM-ER / Excalibur / GLSDB precision degraded.
- Both sides race to inertial / multi-sensor fallbacks.

BALTIC & NORDIC

Daily weather

- Finnair suspends Tartu (Estonia) flights, Apr–May 2024. Estonian, Finnish, Latvian governments publicly attribute jamming to Russia.
- Kaliningrad and Pskov as the structural source.

EAST MED & RED SEA

Aviation-grade spoofing

- Hundreds of commercial-aviation spoofing events since Sep 2023 (OPSGROUP / IATA).
- Tel Aviv approach, Cairo, Beirut, Baghdad corridors.
- Flight-management systems mis-positioned.

HIGH NORTH & SPACE

The contested orbit

- Russia's Kosmos-2576 (May 2024) co-orbital inspection of US NRO assets.
- Persistent Bardufoss / Banak / Finnmark interference (Norwegian authorities)
- Submarine cable fragility.

Legacy GNSS is a 1990s architecture in a 2026 war

Below the noise floor. Asymmetric. Unauthenticated at the ranging level. Replenished in decades.

ATTRIBUTE	LEGACY MEO GNSS	AUTHENTICATED LEO PNT
Orbit altitude	20,200 km (GPS) · 23,200 km (Galileo)	600–1,500 km → 15–30× closer
Received signal power	≈ −158 dBW · below noise floor	+30 dB stronger; 100–1,000× link budget
Authentication	OSNMA on Galileo (msg only); none on GPS L1 C/A	Per-frame cryptographic + Doppler signature
Replenishment cycle	10–15 yrs (Block IIIF, Galileo G2 ~2030)	1–3 yrs · software-defined payloads
Time-to-first-fix	30 s – several min (cold)	< 5 s; PPP convergence 1–5 min vs. 15–30
Jam to deny at 100 km	≈ 200–500 W (legacy GPS)	10–40 kW required (orders of magnitude harder)

INTERFERENCE ASYMMETRY

Attacker

Commercial GPS jammer	**€20 – €200**
SDR spoofer	**< €500**
Military jammer	**€5 – 50 k**

Defender

CRPA antenna	**€50 – 200 k**
INS / GNSS hybrid	**€100 k +**

…and capability still lost in a strong EW environment.

This is not a price problem. It is an architecture problem.

OSNMA on Galileo is operational and important — a critical first step, but message-only and rate-limited. It does not authenticate the ranging signal itself.

Four layers of a hardened digital border

Cyber–geospatial convergence is not a product. It is a stacked architecture.

01

AUTHENTICATED LEO PNT

- Cryptographic per-frame signal authentication on a LEO constellation.
- Doppler-driven integrity (±40–60 kHz).
- The trust root for everything that moves, navigates, or fires.

02

ZERO-TRUST GEOINT PIPELINE

- Identity, attestation and policy at every hop from sensor to shooter.
- No node trusted because of its IP.
- No data trusted because of its label.

03

PROVENANCE & ATTESTATION

- Cryptographic content credentials (C2PA-class) on every image, every track, every observation.
- Defends against AI-generated geospatial deepfakes — already demonstrated in the literature.

04

POST-QUANTUM READINESS

- Long-lived keys on satellites, weapons, comms must migrate now.
- Adversaries are already harvesting; the decryption is just a date on a calendar.

Remove any one layer and the whole border is theatre.

Layered PNT Architecture – LEO's Role in the Overall System

LEO-PNT does not replace GNSS – it complements and serves as an integrity verifier. Resilience emerges from the combination of independent layers:

LEO-PNT — Sovereign, encrypted, jam-resistant. Independent time source.

GNSS (MEO) — GPS, Galileo (+ OSNMA), GLONASS, BeiDou – multi-source tactical level.

Inertial Systems — INS / AHRS – short-term autonomy without external signal.

Network-based — 5G/6G TDoA, eLoran, opportunistinen LEO (Iridium STL, Starlink).

Sensor Fusion — Computer vision (VIO/SLAM), terrain matching, magnetometer, celestial navigation.

A weakness at one level does not bring down the whole. LEO-PNT adds a geometrically and signal-independent layer to the architecture.

What it looks like when you actually build it

Sharpnav · ESA Phi-Lab LEOnhard · TRL-5 demonstrator · Aalto / FGI / Tampere research base.

Traditional GNSS constellations

- Satellites in Medium Earth Orbit
- Altitude ~ 20 000 kilometres
- Time to first fix typically between 10-115 seconds
- Signal is very prone to interference, leading to signal loss within buildings & busy cityscapes

LEO-PNT constellations

- Satellites in Low Earth Orbit
- Altitude 600 – 2000 kilometres
- Significantly faster time to first fix compared to traditional systems
- Up to **100x signal strength** with same transmitted power compared to GNSS
- Significantly lower latency & shorter convergence times due to quickly changing signal paths
- Multi Band L+C

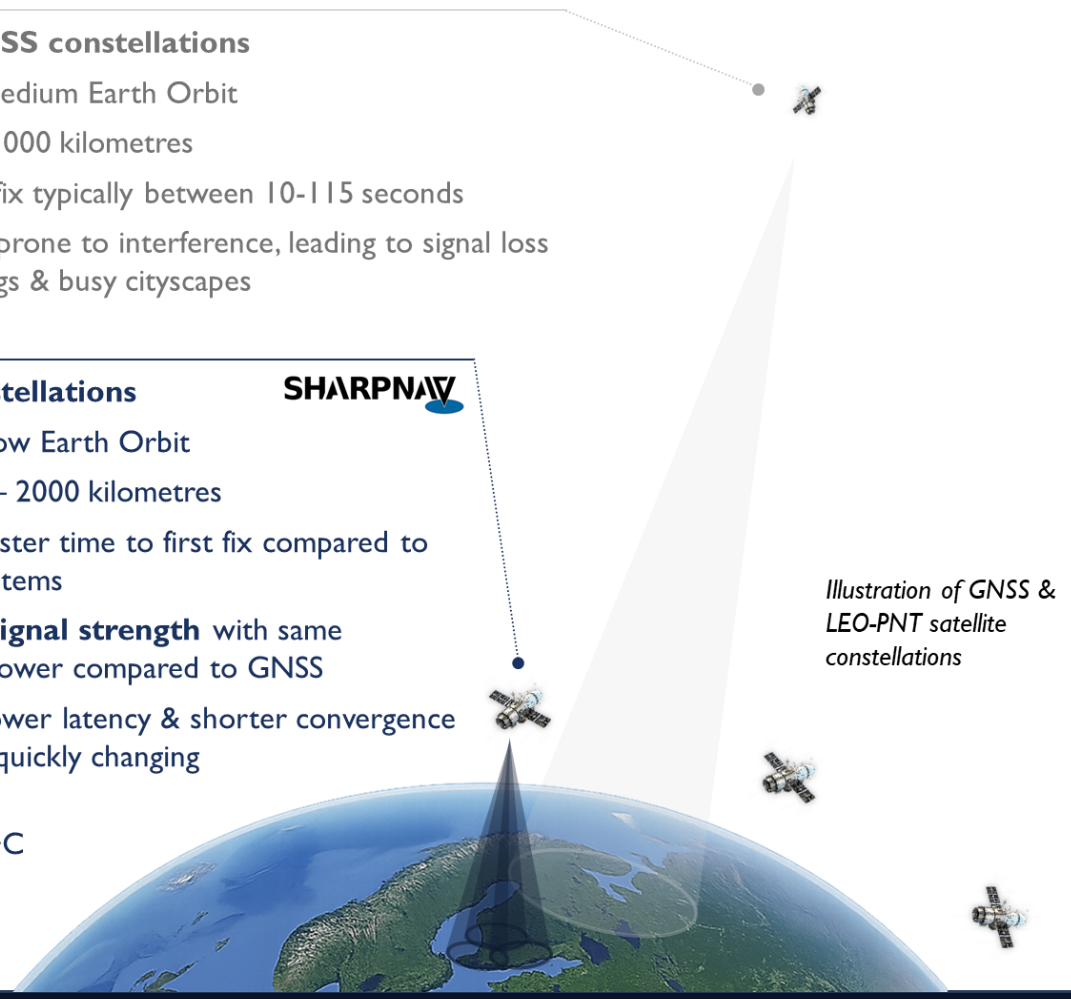


Illustration of GNSS & LEO-PNT satellite constellations

PHASED DEPLOYMENT — NORDIC FIRST

PILOT · 2026–2028
4 satellites · technology validation · Nordic coverage

OPERATIONAL · 2029–2030
~50 satellites · regional service · defence-sector entry

GLOBAL · 2030–2032
~300 satellites · global coverage

DESIGN PRINCIPLES

- Survives EW · +30 dB margin
- Latency fits autonomous decision loop
- Sovereign keys · no foreign master switch
- New Space economics · not exquisite

Space as an Enabler