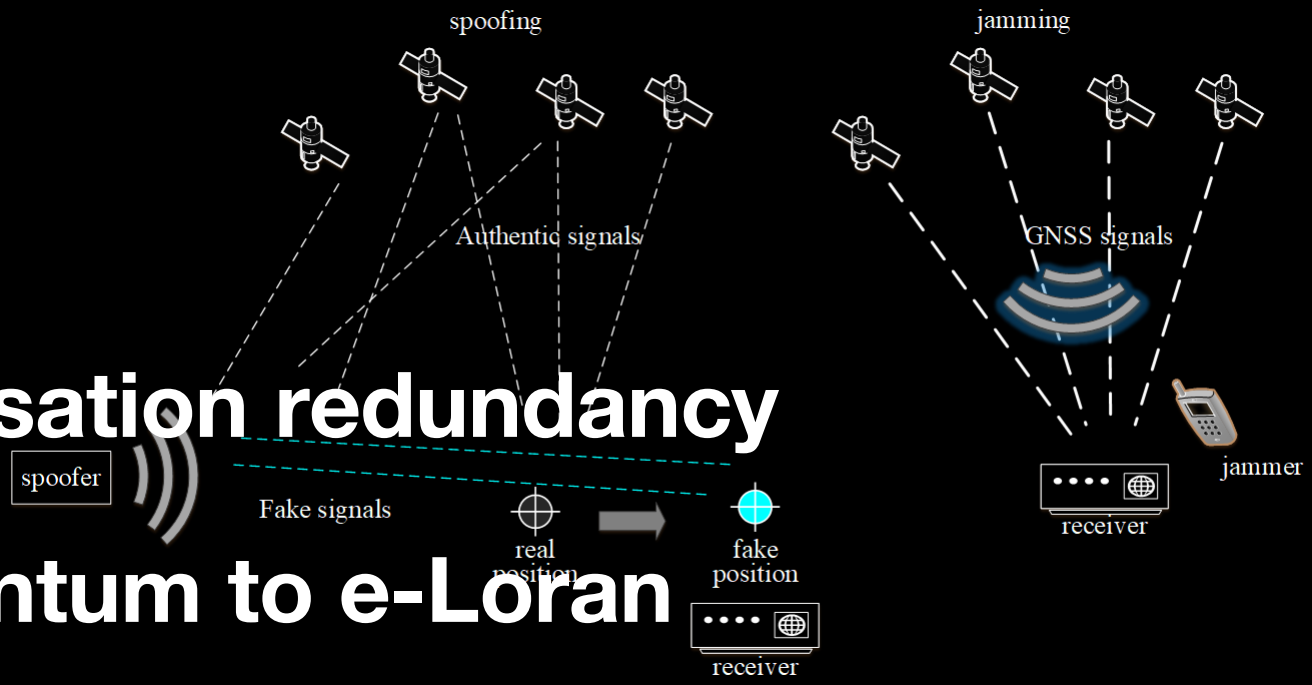
Orange
Innovation



Synchronisation redundancy for Telcos From Quantum to e-Loran

Olivier Le Moult
ORANGE INNOVATION NETWORKS
October 8, 2025

Orange Expert Future networks

orange™

Summary

1 - GNSS Vulnerabilities Panorama

Global Navigation Satellites Systems (GNSS) deliver L band signals for positioning, navigation and timing needs for all types of final users.

These services are mainly confronted with four types of threats:

1

Environnement

Mainly Space Weather plus Terrestrial Environnement

2

Unintentional

Interferences, harmonics

3

Intentional

Jamming, spoofing

4

Receiver

Mainly IT security topics

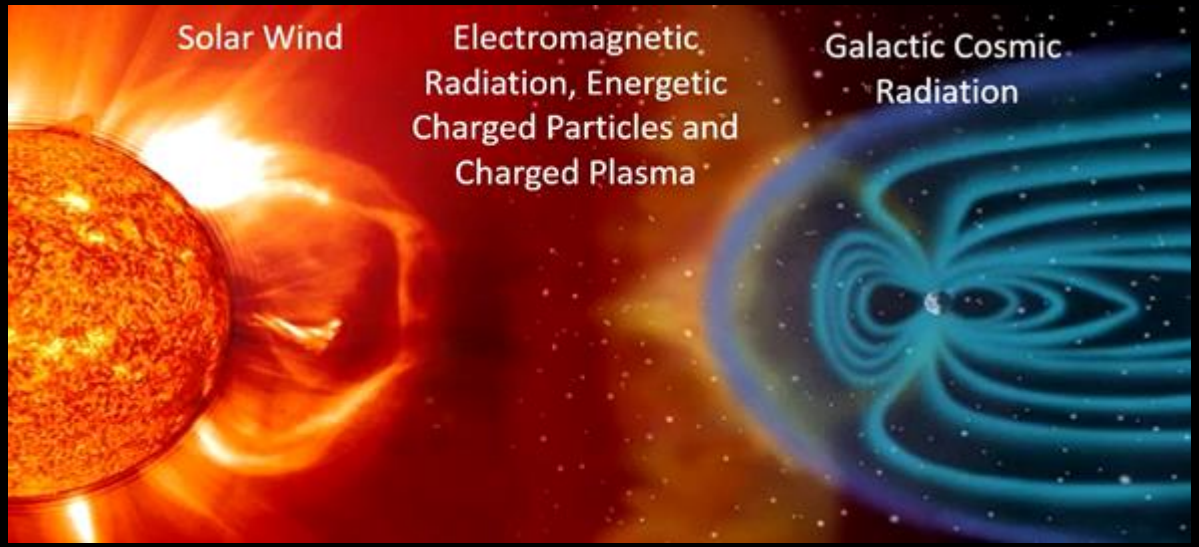
Summary

1. GNSS – Vulnerabilities Panorama
2. GNSS – Vulnerabilities basics
3. Current situation – Space Weather
4. Current situation – Jamming-Spoofing
5. Conclusion

1 - GNSS Vulnerabilities basics – part 1

GNSS signals come from very distant satellites (20000-23000 km MEO constellations)

The first vulnerability are the hazards from space weather, mainly due to Sun behavior:



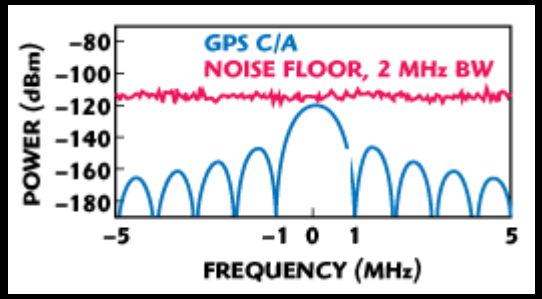
The main consequences are proper functioning of satellites, ionospheric perturbations and Geomagnetically Induced Currents (GICs).

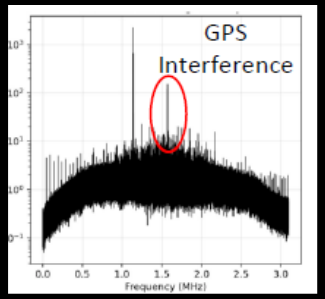
Ionospheric disturbances can momentarily modify the performance of GNSS receivers used in telecoms.

1 - GNSS Vulnerabilities basics – part 2

GNSS signals have also common vulnerabilities, due to their design.

The second vulnerability (Jamming) is due to the level of received signals, below thermal noise power:





GPS main civil signal C/A power level and interference example

The consequence is that GNSS signals are very easily affected by interferences in their useful bandwidth or jammed by malicious RF transmitters.

The third vulnerability (Spoofing) comes from the original GPS civil signal, which is easily generated by malicious emitters near the users receivers.

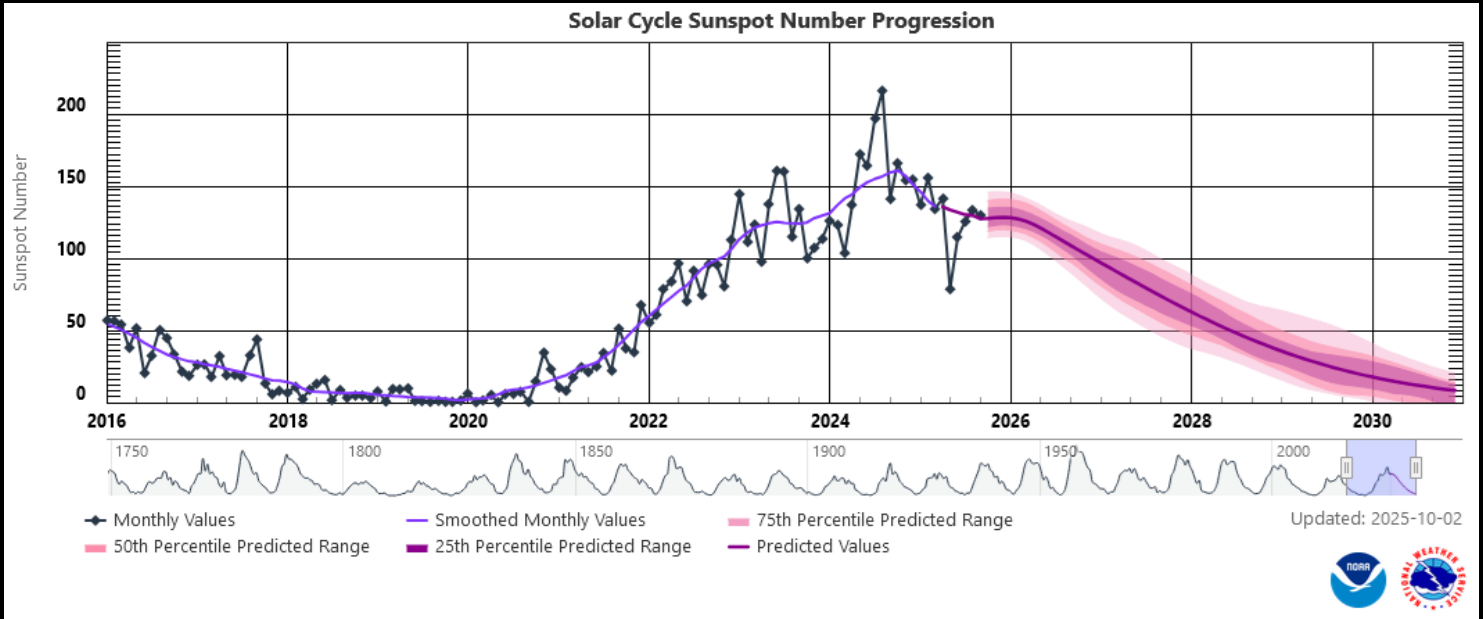
The goal is to deceive honest GNSS receivers by transmitting erroneous data with more powerful fake signals.

Summary

1. GNSS – Vulnerabilities Panorama
2. GNSS – Vulnerabilities basics
3. **Current situation – Space Weather**
4. Current situation – Jamming-Spoofing
5. Conclusion

3 – Current situation – Space Weather part 1

The main concern was the Sun maximum activity for its 25th cycle (11 years periodic activity cycles):



Among the many models, maximum activity was somewhere in 2025, last G4 event was June 2, 2025.

In this figure, the number of Sunspots is directly linked to possible Solar Storms reaching the Earth.

3 – Current situation – Space Weather part 2

The better example was the G5 event (May 11, 2024):

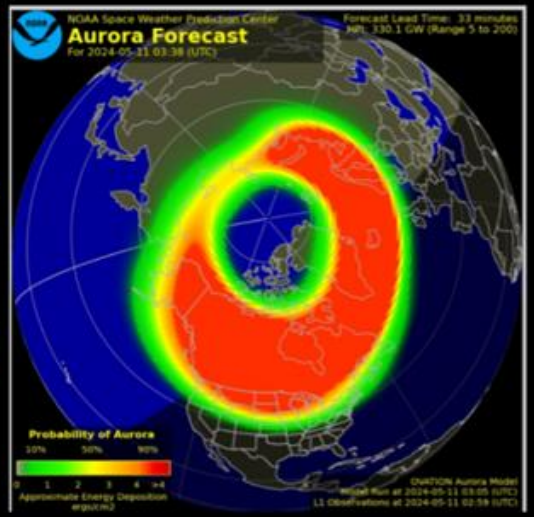
G5 KEY MESSAGES

Extreme (G5) conditions were observed again at 1128 UTC (0728 EDT), and storming of varying intensity will persist through at least Sunday.

The threat of additional strong flares and CMEs will remain until the large and magnetically complex sunspot cluster (NOAA region 3664) rotates out of view over the next several days.

There have been reports of power grid irregularities and degradation to high-frequency communications and GPS.

Overnight, aurora were visible across much of the United States. Weather permitting, they may be visible again tonight.



Index	MAY 2024	OCT 2003	MAR 1989	MAY 1921	SEP 1859
Disturbance Storm Index (nT)	-412	-383	-589	~ -907	~-1200
A_p-Index	271	204	246	NA	NA

G5 is the highest category for Geomagnetic events impacting Earth, but in May 2024, the impact was not very high, 3 times lower than the 1859 Carrington Event.

Since 2024, others energetic events took place, Solar Cycle number 25 maximum was in 2025.

Summary

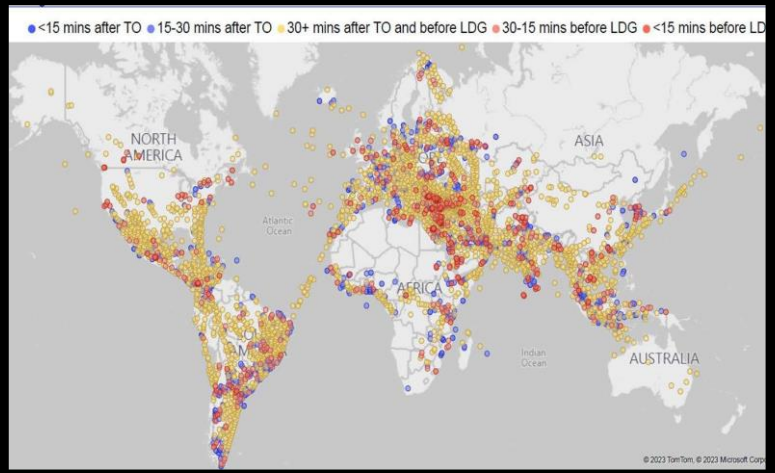
1. GNSS – Vulnerabilities Panorama
2. GNSS – Vulnerabilities basics
3. Current situation – Space Weather
4. Current situation – Jamming-Spoofing
5. Conclusion

4 – Current situation – Jamming

GNSS is easily jammed, simple jammers are easy to find on internet:

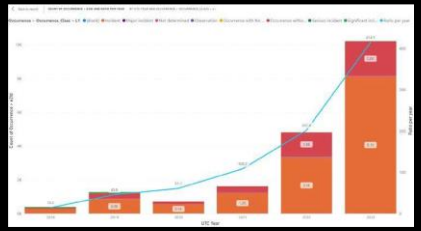
The level of hazard is much higher due to wars in Ukraine and in Middle-East.

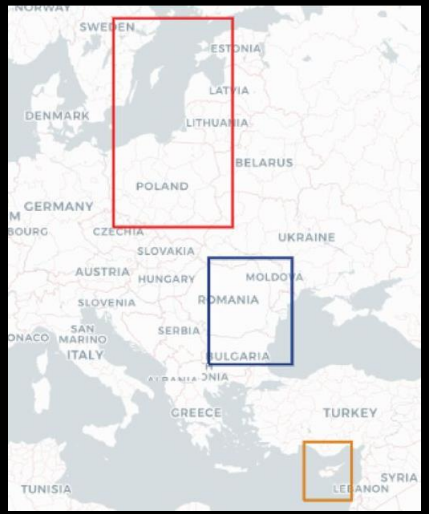
Easily viewed in civil aviation navigation perturbations (until 2023):



Jam.

Events:





Above: June 2022-June 2023: 209 Airlines recorded ~150,000 Loss of GPS. **65%** increase in GPS loss rate for **2024** – IATA

Degraded GNSS for telcos near the “hot” boundaries, for example in East and Central Europe and Middle-East.

4 – Current situation – Jamming part 2

Significant spread of long range GNSS jammers in Europe :

For Baltic Sea, from Russian Kaliningrad Jamming system, see annex 1.

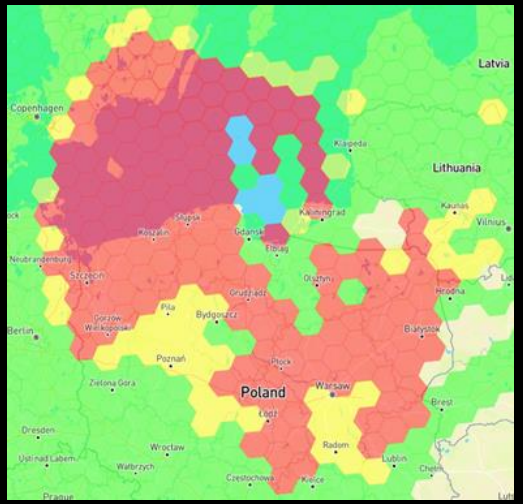
December 26, 2023 widest Jamming event in Europe, zoom below:

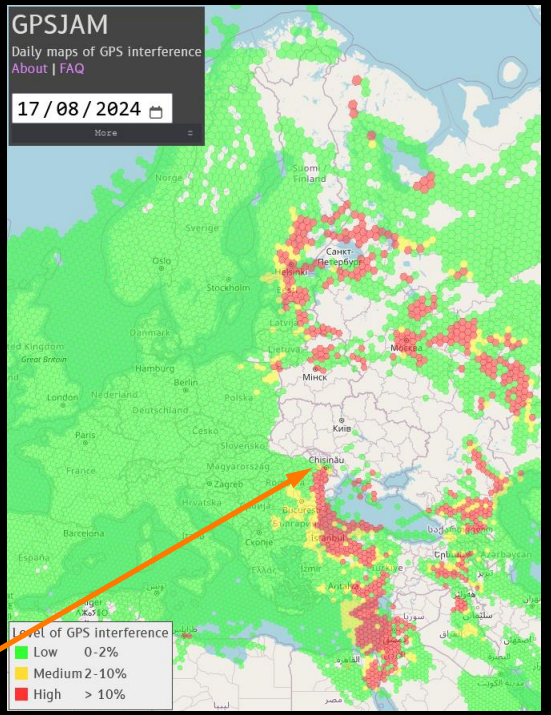
Copenhagen

Latvia

Lithuania

Poland





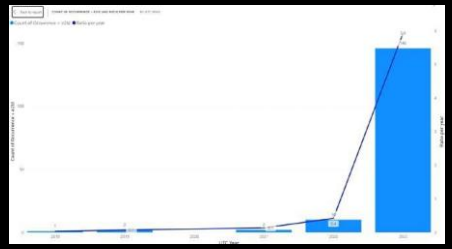
For ORANGE, GNSS devices impacts in Poland, Romania, Moldavia up to the loss of GNSS receivers locks.

These disturbances are often linked to other aggressive actions (spoofing, other RF bands jammed,…)

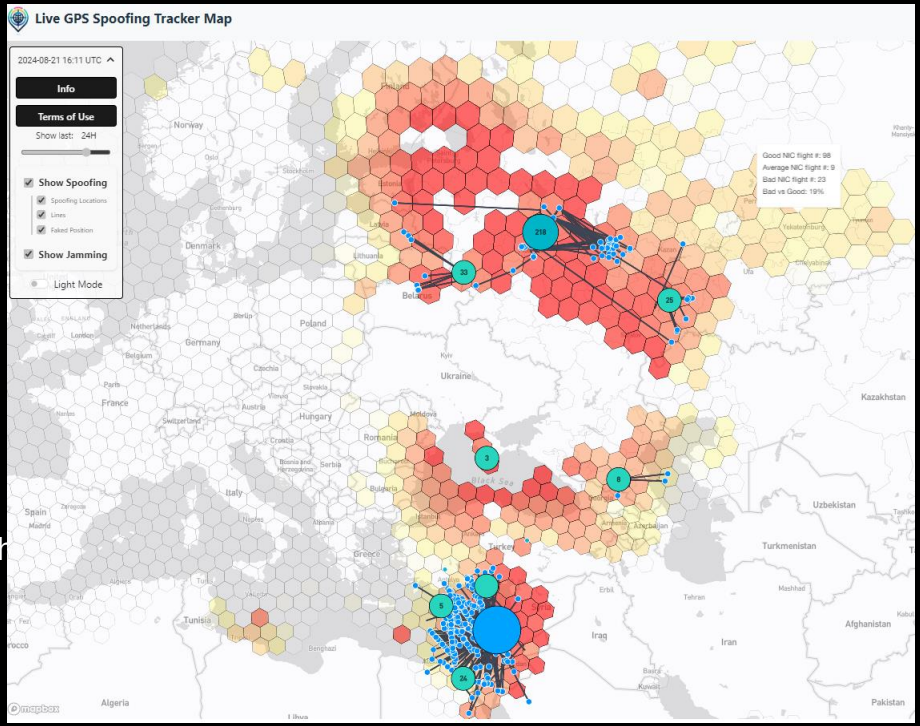
4 – Current situation – Spoofing

GPS basic civil signal (C/A) may be spoofed, now with **SDR** (Sofware-Defined Radio) products, as jamming/.
It is possible to emit forged navigation messages to counterfeit positioning and timing in remote receivers.
The use of SDR spoofing emitters facilitates to attack modern GNSS signals (GPS L5, Galileo…).
Easily viewed in civil aviation navigation perturbations.

Spoofing events
Until 2023 :



Right map estimates spoofing events as detected by commercial aircrafts navigation equipment, for 20-21, August 2024 (24 h means).
No data from war zones and their surroundings as civil air traffic is not authorized. In fact, the website uses **ADS-B** measurements, wh means potential navigation system interference.



4 – Current situation – Spoofing part 2

The more economical threat for spoofing is the **meaconing** method:
It is an adaptation of a GNSS receiver to be used as a “rebroadcaster”, emitting shifted information in its zone.
The simplest form is the well-know use case of GNSS repeaters, already in legal use for many years.
If the repeated GNSS signal is sufficiently delayed, legal receivers can be impacted for time processing.

The Spoofing threat is not only in delivering false positioning, but also malicious timing information.

Civil Aviation tragic case was the Azerbaijan Airlines flight 8243 on 25 December, 2024, see also this article:

> Aviation’s Hidden Threat - How GPS Spoofing Endangers Flights Worldwide 08/01/2025
> https://www.forbes.com/councils/forbestechcouncil/2025/01/08/aviations-hidden-threat-how-gps-spoofing-endangers-flights-worldwide/

Official UNO agencies call against GNSS threats: 18/03/2025 / ICAO-IMO-ITU-Joint-Statement 2025
https://www.itu.int/en/mediacentre/Documents/2025/ICAO-IMO-ITU-Joint-Statement.pdf

Summary

1. GNSS – Vulnerabilities Panorama
2. GNSS – Vulnerabilities basics
3. Current situation – Space Weather
4. Current situation – Jamming-Spoofing
5. Vulnerabilities ecosystem evolution
6. Conclusion

5 – Vulnerabilities ecosystem evolution

USA:

After many years of activities, **Complementary PNT (CPNT)** program is launched since September 2023.

Firsts Calls for Proposals: Two in 2024, funding: only 15 M$. US Senate is pushing for official review from DHS by February 2025 for US GPS vulnerabilities mitigations. See Annex 2.

Europe:

NAVigation Innovation Support Programme Advisory Committee (NAVAC) "**PNT Vision 2035**" report:

Delivered in March 2024, mix of Advanced PNT solutions and major Complementary PNT: Ground PNT.

First request for proposals in preparation. Note: UK launches commercial e-Loran service. See Annex 4.

France:

Previous important report: Impact study of the loss of GNSS signals, 2022.

"Brainstorming" in France: From low cost (possible adaptation for 162 kHz signal from Allouis ?) to more ambitious ones (GNSS-like LEO satellites,…). The SCPTime offer is now with EASii IC firm, Grenoble: a secured and traceable NTP delivery service.

5 – Vulnerabilities ecosystem evolution part 2

USA:

Complementary PNT (CPNT) alternatives: complementary LEO constellation (Resilient GPS, **R-GPS** phase 0) and long term successor of GPS satellites, terrestrial solutions (RF beacons, eLoran, signals of Opportunity, SoP: Digital Broadcasting, 5G, optical fiber distribution, …) plus IEEE P1952 – Resilient PNT User Equipment.

Europe:

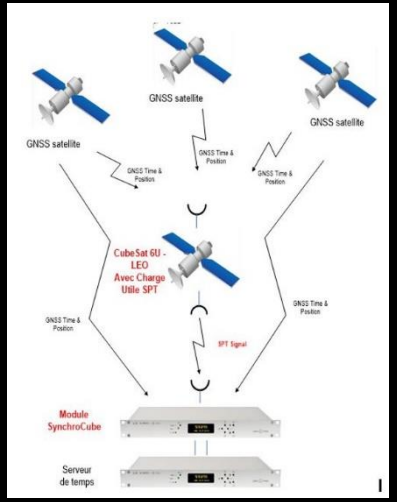
NAVAC "**PNT Vision 2035**" report: sudden lack of GNSS in Europe will mean losses of tens of billions per day.

For Timing, proposals for a more resilient Galileo (e.g., OSNMA feature, complementary LEO satellites) and a new European Timing service.

France:

Space: SynchroCube project, LEO satellite to complement GNSS signals, more powerful, demonstrator satellite launched and preliminary tests in 2025, figure at the right:

Terrestrial : SCPTime (EASii IC), in the future: T-Refimeve.



5 – Vulnerabilities ecosystem evolution part 3

GNSS redundancy exemplary cases:

E-Loran alternative: Modernization for Loran-C and previously Loran technology (WW2, Long Range Navigation, Hyperbolic navigation solution from very low frequency/very long range radio (100 kHz) beacons).

The Loran technology has not been operational in the USA or Europe for about 10 years. It has been modernized with **e-Loran**, which is used in the UK, South Korea and the Middle East.

UK tries to convince some European countries to reinvest in this “very-hard to jam” technology, see Annex 4.

Recent understanding document between UK and France, for several technological topics including PNT resiliency/redundancy :

https://www.gov.uk/government/news/uk-and-france-partner-on-navigation-systems-to-protect-critical-infrastructure-from-hostile-threats

Loran-like technology use in China as nation-wide Beidou redundancy solution and use in Russia with Chayka, including in war.

Quantum solutions:

Many technological approaches for Quantum Synchronisation Solutions, with partial redundancy capability for GNSS vulnerabilities, see Appendices.

Summary

1. GNSS – Vulnerabilities Panorama
2. GNSS – Vulnerabilities basics
3. Current situation – Space Weather
4. Current situation – Jamming-Spoofing
5. Vulnerabilities ecosystem evolution
6. Conclusion

6 – Conclusion

GNSS vulnerabilities are addressed by most developed countries, especially USA, Europe, UK and Asia.

Important Space Weather events in the past (1989, 2003…) have already brought precaution for energy networks and satellites, but the G5 event (May 2024) was a small one, the **25th Solar Maximum** is gone.

Warning: It is important to underline that the maximum activity peak in a Solar Cycle is not the only period for massive Space Weather events, they can appear in a minimum activity period as well, with lower probability.

Jamming and Spoofing events are numerous (wars in Ukraine and in Middle-East), and the massive use of powerful jammers, plus generalization of inexpensive jammers. The concerning fact is the worldwide use of spoofing, as underlined by Civil Aviation authorities. Both convinced the EU to launch "**e-GNSS**" project.

A disturbing fact is the generalization of **e-Loran**-like projects, for example in Russia and China, to prepare for a future situation of generalized unavailability of GNSS signals. Another path is quantum-enhanced solutions.

To conclude, there are many redundancy/complementary projects to have more resilient PNT services. Terrestrial solutions compete with LEO projects, with the advantage of long experience in scientific domains for optical fibers solutions. A 5G/6G-enabled future timing service will be a great opportunity for **ORANGE**.

7 – Annex 1

Focus on main Russian GNSS Jamming/spoofing installation in Europe:
Kaliningrad, North of Poland border, Russian exclave of 15000 km^2, heavily militarized.

Top right photo is the Center highest antenna viewed from railway:
Right figure is a rough radiohorizon versus loss of signal for planes, crossing of circles is Kaliningrad, right picture:

Exact range of possible jamming is not known, about 300 km for military special trucks,
Russian Krasukha-4 jammer:
If Russia jams wide aeras, they have less precise navigation solution with **Chayka** (Loran) for military use.

7 – Annex 2

USA Focus: Tests of different redundancy-resiliency GNSS solutions, 2020.

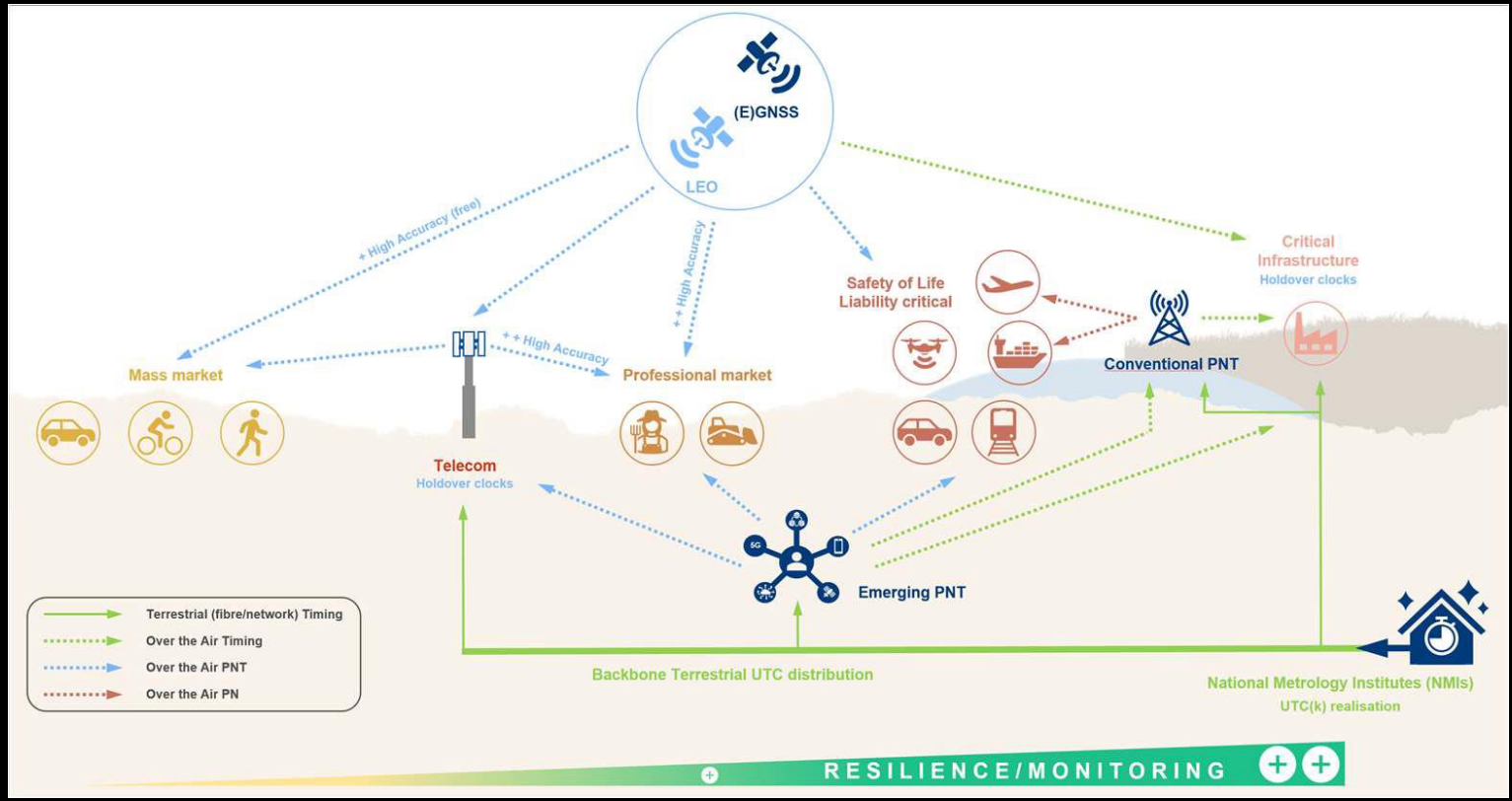
PNT Technology Vendor	Demo Site	72-Hr Bench Static Timing	Static Outdoor Timing	Static Indoor Timing	Static Basement Timing	Reference Station Offset (eLoran Timing)	Dynamic Outdoor Positioning with Holds	Static Outdoor Positioning	Static Indoor Positioning	Airborne Positioning
Echo Ridge LLC	LaRC					N/A		self-sync		
Hellen Systems, LLC	JBCC	UTC			UTC	UTC				
NextNav LLC	LaRC	cascade	cascade	cascade	cascade	N/A	cascade	cascade	cascade	cascade
OPNT B.V.	LaRC	UTC				N/A				
PhasorLab Inc.	JBCC	cascade	cascade	cascade		N/A	cascade	cascade		cascade
Satelles, Inc.	JBCC	UTC	UTC	UTC	UTC	N/A		UTC		
Serco Inc.	JBCC					N/A	cascade	cascade		
Seven Solutions S.L.	LaRC	UTC				N/A				
Skyhook Wireless, Inc.	LaRC					N/A	self-sync	self-sync	self-sync	self-sync
TRX Systems, Inc.	LaRC					N/A	N/A	N/A	N/A	
UrsaNav Inc.	JBCC	UTC		UTC	UTC	UTC				
GPS (SPS PS)	All	UTC	UTC			UTC	UTC	UTC		UTC

Rubric:
- UTC
- cascade
- self-sync

Service Synchronization Consensus Scorecard - 2021

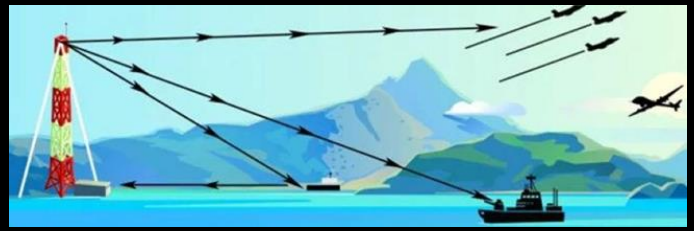
7 – Annex 3

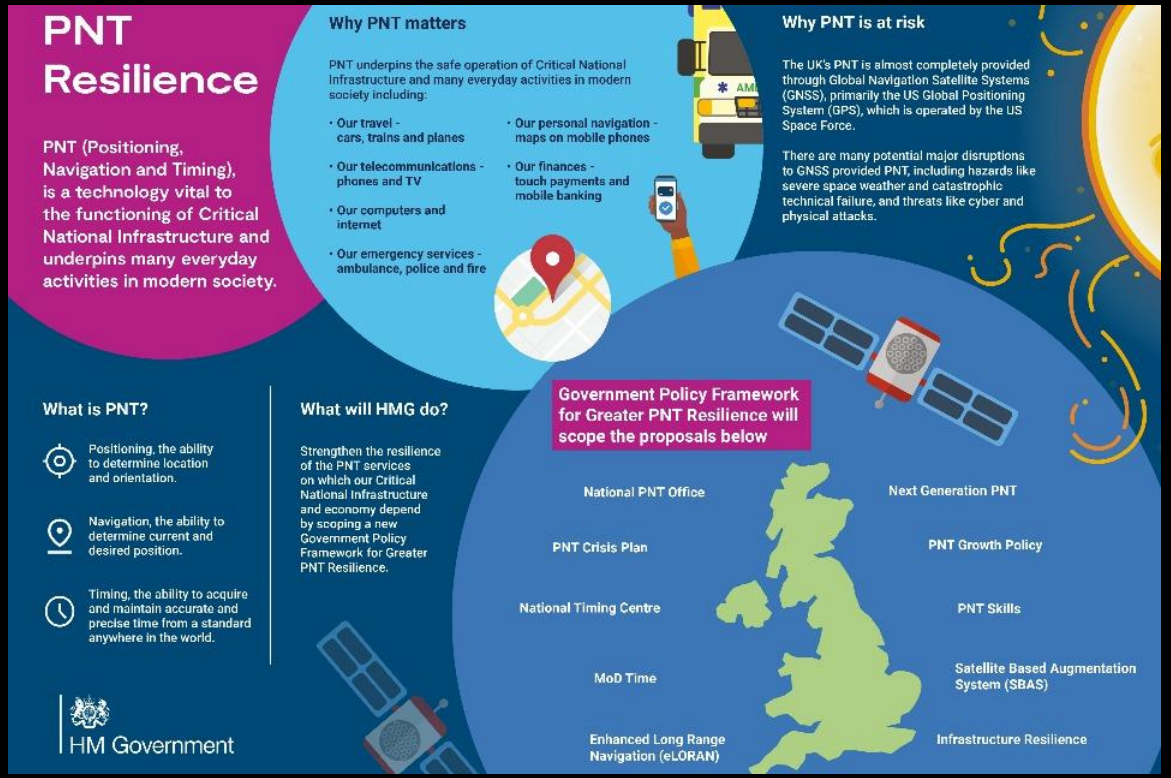
Europe Focus: **C-PNT : Terrestrial Time Backbone** Service Operations Research Contract, architecture:



7 – Annex 4

UK Focus: National Timing Infrastructure, including e-Loran (100 kHz, 1 MW, very long range):





8 – Acronyms & links

ADS-B: Automatic Dependent Surveillance – Broadcast (Aviation)

A-GPS, A-GNSS: Augmented, Assured, Alternate GPS/GNSS

C/A: Coarse Acquisition (GPS L1 C/A signal)

E-Loran: Enhanced-LOng-RAnge Navigation

EW: Electronic Warfare

LEO: Low Earth Orbit

OSNMA: Open Service Navigation Message Authentication

PNT: Position, Navigation and Timing

SW: Space Weather

NAVAC PNT Vision 2035: https://navisp.esa.int/uploads/files/documents/NAVAC%20White%20Paper%20May%202024.pdf

US Senate DHS letter, Dec. 18, 2024: https://www.hassan.senate.gov/imo/media/doc/dhs_gps_letter.pdf

Resilient Positioning, Navigation, and Timing; DHS: https://www.dhs.gov/sites/default/files/2022-06/22_0609_st_resilient_pnt_ra.pdf

IEEE P1952 Resilient Positioning, Navigation and Timing (PNT) User Equipment : https://sagroups.ieee.org/p1952/

Galileo OSNMA: https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma

GPS Backup Technology Demonstration report, 2021:
https://www.transportation.gov/administrations/assistant-secretary-research-and-technology/complementary-pnt-and-gps-backup

Orange
Innovation

Thanks

Especially for FIRST-TF organisers and for the funding of the mission.
And for the warm welcome of FOTON institute and rich laboratory visits ☺

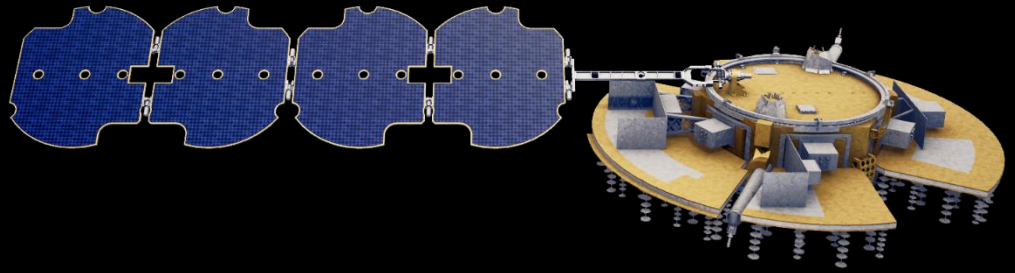
Olivier Le Moult : olivier.lemoult@orange.com

orange™

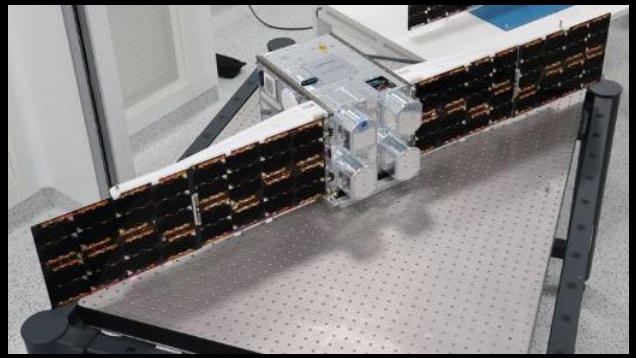
9 – Appendices – 1.1

Recently new opportunities for **Space-based** Time and Frequency sources:

USA NTS-3 - Demonstrator for future GNSS satellites, beyond/supplemental to GPS, launched August 12, 2025 (9 months late):



France - Pandore nano-satellite, SynchroCube Demonstrator, launched about 9 months, see infographic next slide :



9 – Appendices – 1.2

France - Pandore nano-satellite, SynchroCube Demonstrator, only French firms, Infographic :

PANDORE

Identity Card

Name
PANDORE

Asset
Five demonstration encompassed

Operating time
12 mois-extensible

Miniaturized technology

Size - 12U
20x20x30

Weight
18 kg

Partners

SAFRAN

ANYWAVES

comat

MICROTEC
High-Rel Electronics

Mission

In-orbit demonstration innovative payloads to Positioning, Navigation and Timing (PNT).

PANDORE satellite to communicate with ground stations in Toulouse and Rennes

Operation as a service

Our entire procedure process is fully automated and integrated with a dedicated interface for the mission programming of the partners.

Payload

Safran-Space & Anywaves: Positionning, Navigation and Timing
Comat: Reaction wheels and Electric Propulsion with solid metal propellant
Microtec: Power Load Controller Unit

590 km

The Earth and PANDORE once in orbit.

+72 hours

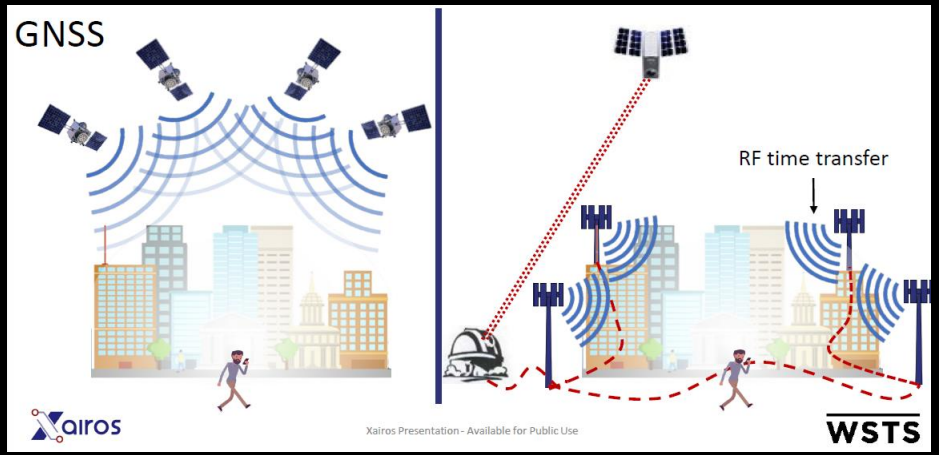
End of early-life operations and start of payload mission testing.

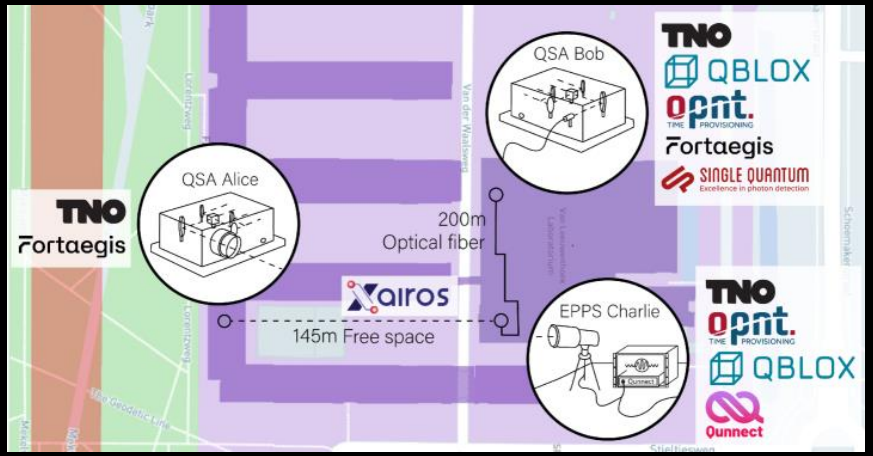
U/SPACE

9 – Appendices – 1.3

Recent new opportunities for **Space-based** Time and Frequency sources:

USA Xairos Systems, Quantum Time Transfer - QTT :





China Micius, quantum synchronisation, few tens of picoseconds: