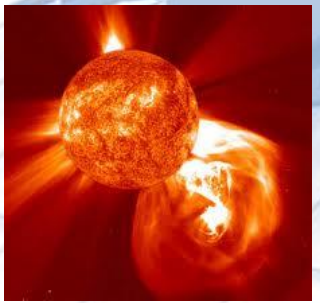
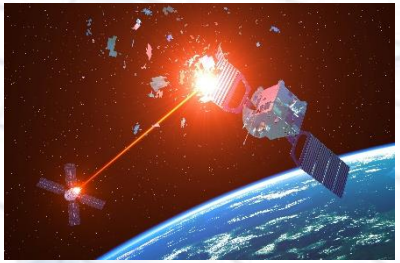
RESILIENT NAVIGATION and TIMING FOUNDATION
Speaking Up for GPS/GNSS Users





Resilient PNT - The Missing Pieces

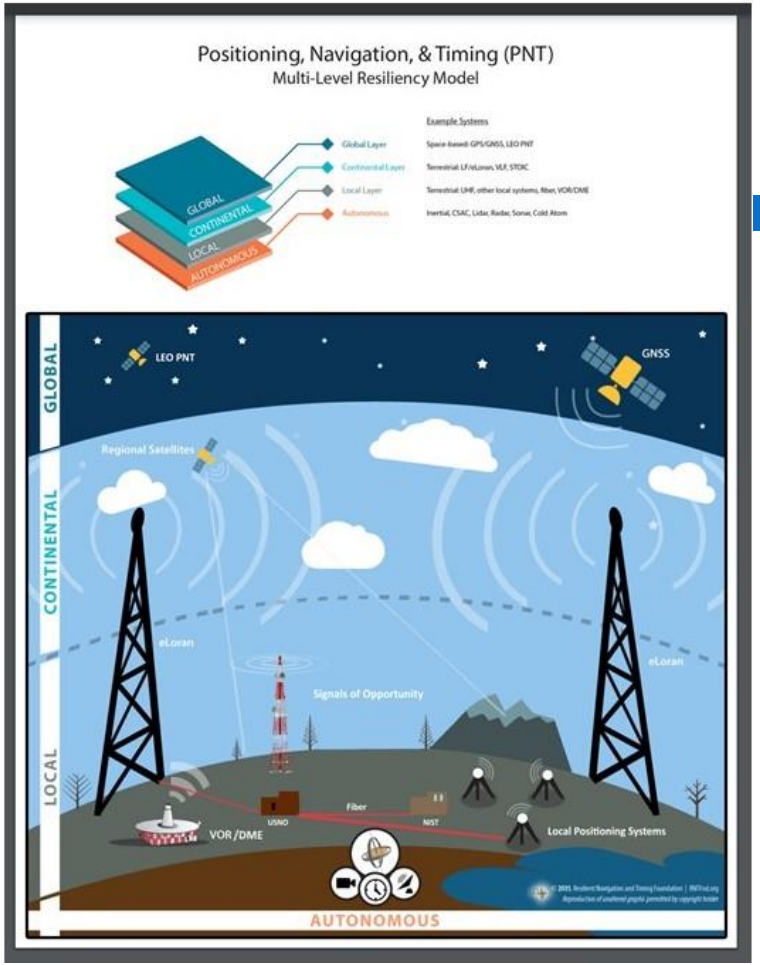
Resilience

Adapt

Withstand

Rapidly Recover

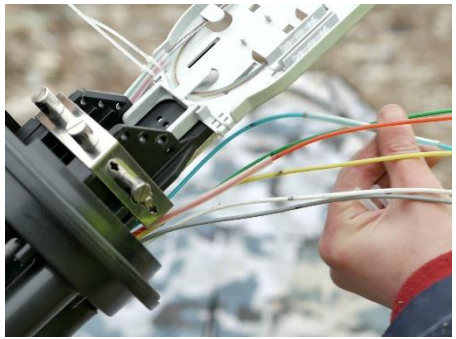
System of Systems



Resilient PNT Triad

RESILIENT NAVIGATION and TIMING FOUNDATION

October 2020



DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA

January 2021

Missing…

Governance

Missing…

Governance

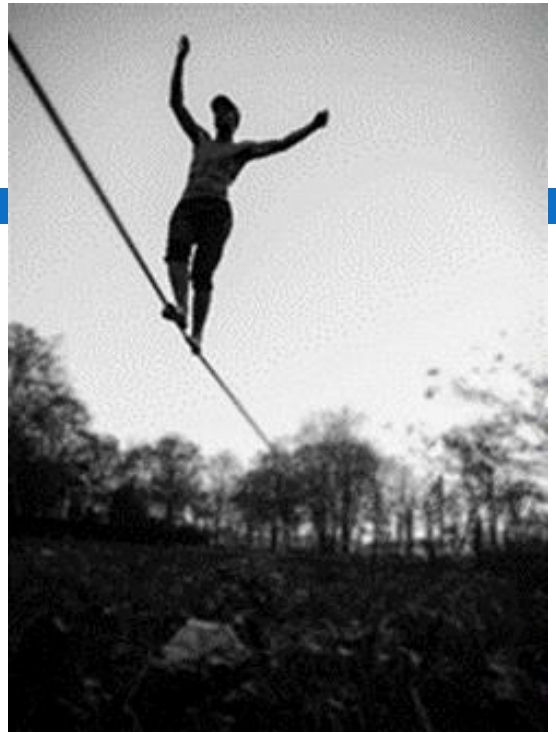
Understanding Risk

Risk =

Threat

Vulnerability

Consequence



Risk

Threat x Vulnerability x Consequence

P(Bad event) x P(damage) x Damage

Risk due wind gust 30kph

P (Threat) 20% x

P (Vulnerable) 10% x

Consequence ($ 15,000) =

Risk = $ 300

Risk (malicious)

Vulnerability x Consequence

x

Threat (Intent x Capability)

Mars Attacks!

Vulnerability — Prob they can easily kill us = 1

x

Consequence — Damage = We all Die

x

Intent — They REALLY want to kill us = 1

x

Mars Attacks!

Capability

No spaceships = 0

Mars Attacks!

Vulnerability = 1 x

Consequence = We all Die x

Intent = 1 x

Capability = 0 .

Risk = 0

GNSS threat vectors

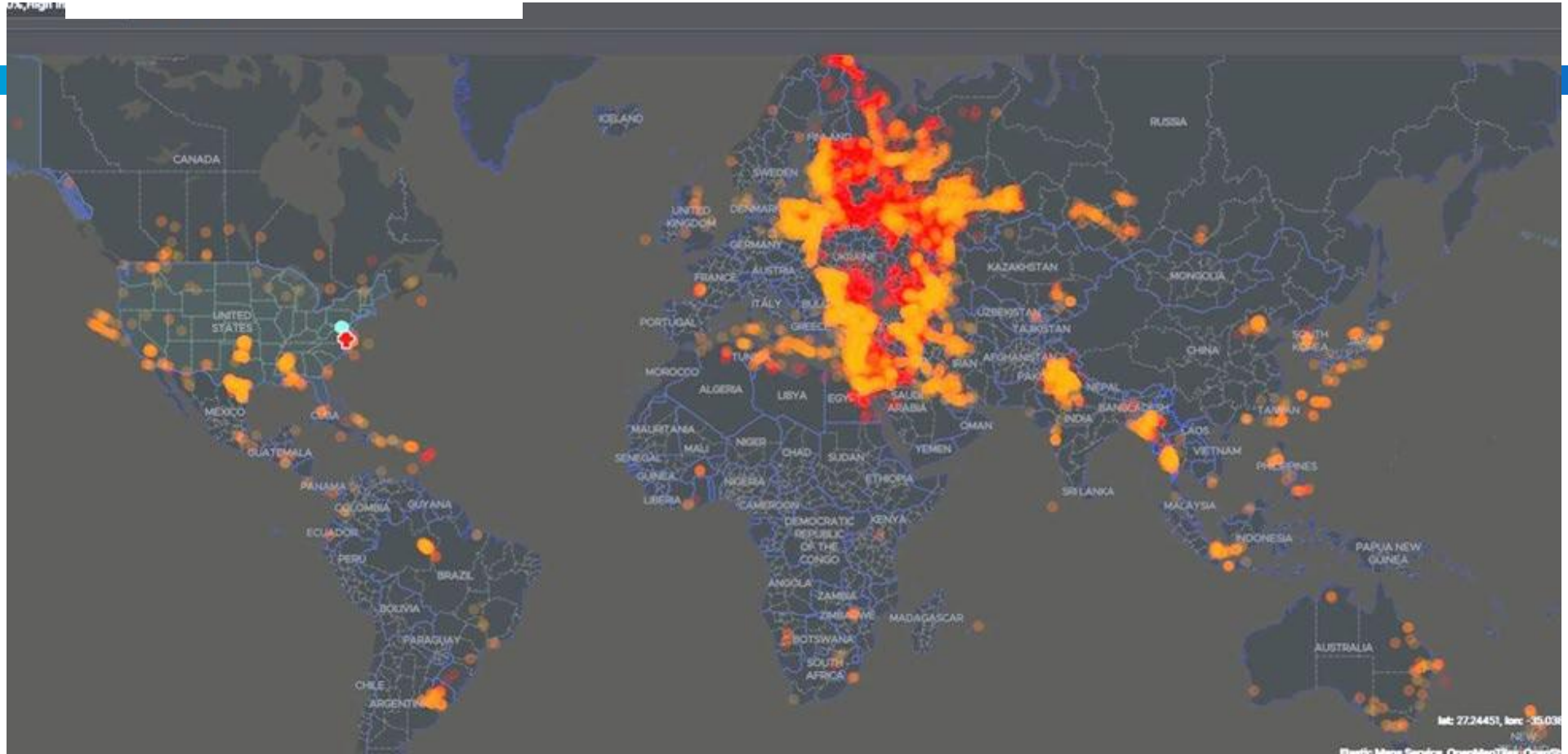
<u>Natural/Accidental</u>

1. Built structure obstruction
2. Terrain obstruction
3. Foliage (pines, hvy canopy)
4. Solar Activity – mild
5. Solar Activity - moderate
6. Solar Activity -powerful
7. Human Error/software
8. Satellite malfunction
9. Control Segment Failure
10. Space Debris
11. Unintentional RF

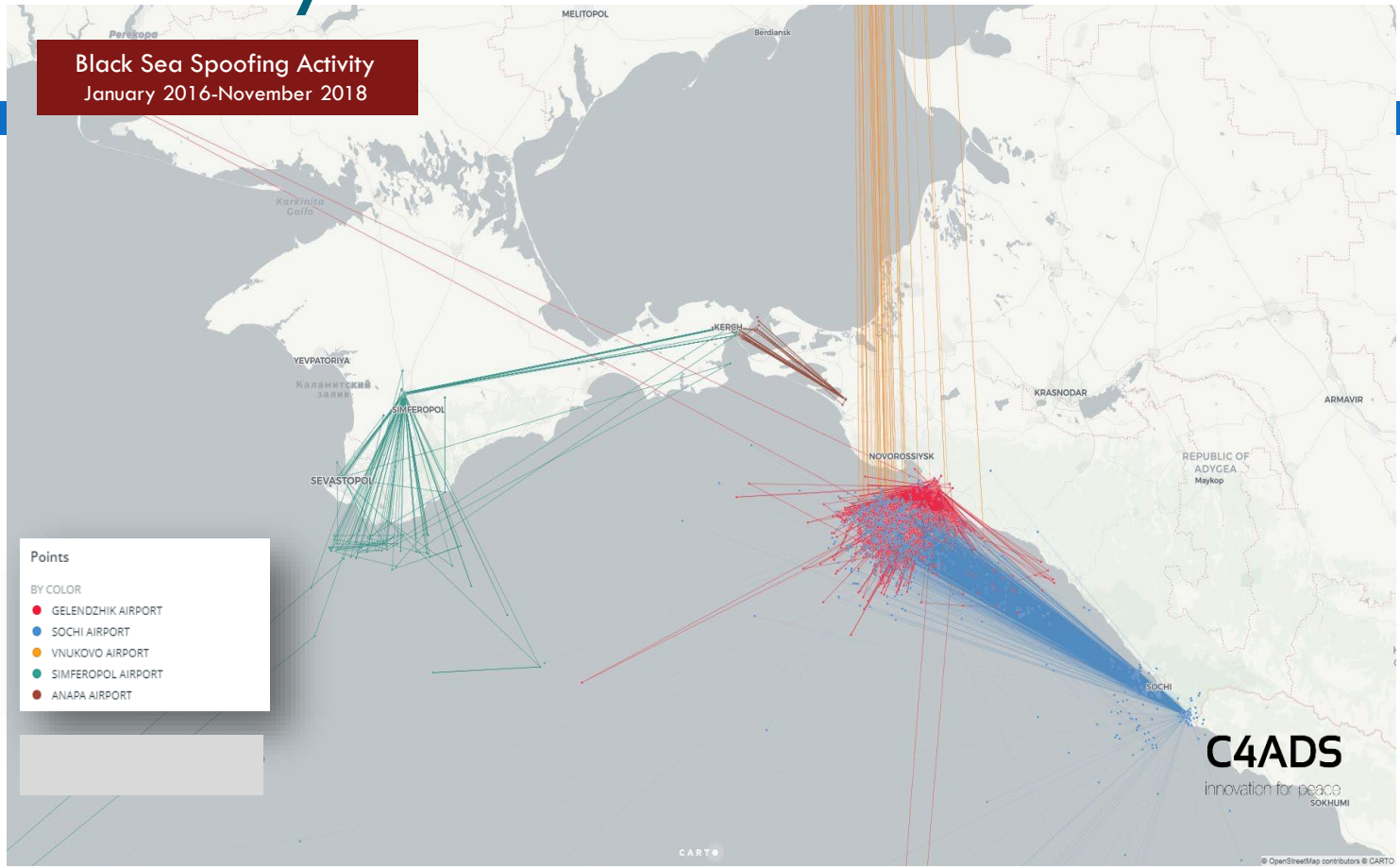
<u>Malicious Acts</u>

12. Privacy seeker (1 event)
13. Criminal Jamming (1 event)
14. Criminal + Privacy 1 Yr Total
15. Criminal Spoofing (1 event)
16. Terrorist Jamming
17. Terrorist Spoofing
18. Military-style Jamming
19. Nat. Agent Spoofing
20. Attack on Satellites
21. Attack on Control Segment
22. Cyber Attack on Control Segment

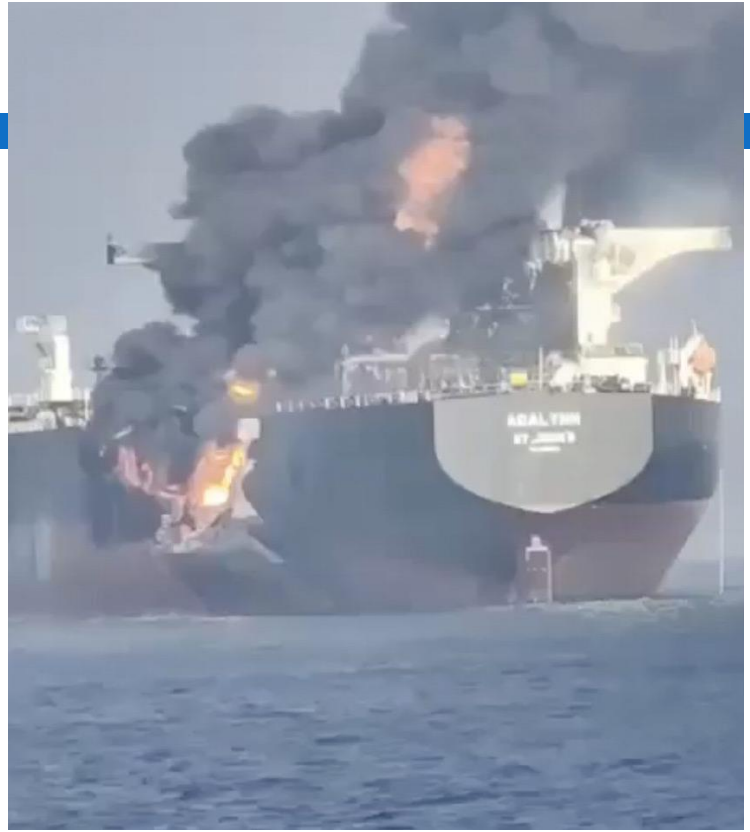
Probabilities



Vulnerability



Consequence



Consequence

Or worse

Do you feel lucky?

Risk = Threat x Vulnerability x Consequence

WASHINGTON VIEW

PNT Threats, Risks and Disaster

Assessing the risk to GNSS and what could happen if we fail to act.

DANA A. GOWARD

In many situations, the biggest threat is not the biggest risk. Failure to understand that and focusing on what appears to be the most pressing concern can lead to disaster.

A classic example is flood preparedness in New Orleans before Hurricane Katrina.

The biggest flood threat to the city has always been frequent intense rains from tropical and other storms. These often overwhelm the city's stormwater management system. Streets and low-lying areas typically flood for a few hours, though sometimes it takes a day or more for the system's pumps and drains to catch up. This happens so frequently it has become a fact of life. Residents have adapted by avoiding low areas and protecting their property as much as possible.

Yet, New Orleans' biggest flood risk has always been a Category 5 Hurricane overtopping and destroying levees. While these storms only strike once every hundred years, their impact is devastating.

Before Katrina, New Orleans had guarded against its greatest flood threat, but not its greatest risk. When Katrina struck, that error cost 3,000 lives and $125 billion in property damage.

PNT Threats and Risks

Localized GPS jamming and spoofing is the biggest threat to PNT services in America and Europe. Local and regional jamming and spoofing has become a fact of life and users are adapting by altering their behavior and, in some cases, upgrading equipment.

The biggest risk to PNT services is by most reckonings some form of long-term GNSS denial. Not the widespread, relatively low impact interference seen today. Yet, it's been a challenge for Western governments to act to avoid a Katrina-like PNT disaster spread across multiple continents, a disaster it will take decades or more to recover from.

Risk Assessment

Structured risk assessments are one way to help leaders and their support staff focus on these kinds of issues.

At a high level, most methodologies assess risk from a potential adverse event as the product of threat: the probability of the adverse event; vulnerability, or the degree the impacted system or population is likely to suffer damage; and consequence, which is the amount of damage likely to occur if no mitigations are in place. Expressed as an equation:

Risk = P(Threat) x P(Vulnerability) x Consequence

The risk equation for potential malicious acts is slightly more complex. Threat is defined as the probability a bad actor can commit the act (capability) multiplied by the probability the bad actor will actually carry out the act (intent). This makes the risk equation for malicious acts:

Risk = Threat (P(capability) x (P(intent)) x P(Vulnerability) x Consequence

Risk Assessment Challenges

Barriers to risk assessment include:

Estimating consequences. A significant obstacle to analyzing larger potential events is the difficulty of predicting

Dana A. Goward is President of the nonprofit Resilient Navigation and Timing Foundation, a public benefit charity advocating for policies and systems to protect GPS satellites, signals and users. He is a member of the President's National Space-Based Advisory Board, and has received multiple international awards for his leadership and advocacy for resilient PNT architectures. Goward is a retired Coast Guard officer and helicopter pilot. In 2013, he retired from the federal Senior Executive Service having served as the maritime navigation authority for the United States.

FIGURE 1 Thirty days of GPS interference in 2024. *Source: US DOT and DOD.*

Inside GNSS+ Nov/Dec 2025

Missing…

Governance

Governance

Structure/ process

Policy myths

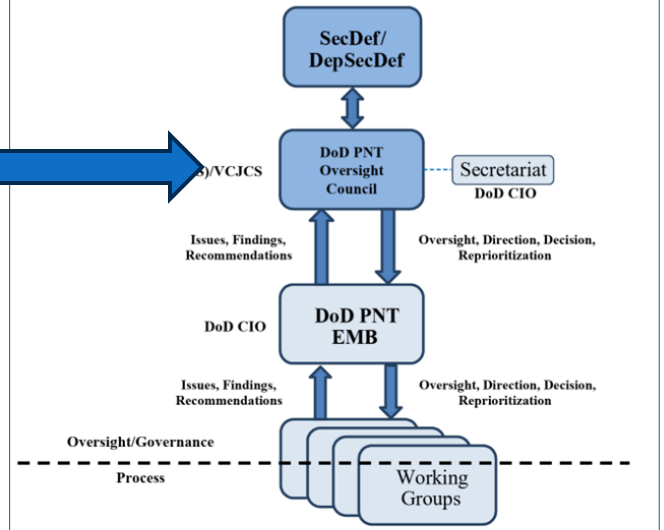
Structure/ Process

Department of Defense/War PNT Oversight Council

Voting Members
(1) Secretary of the Army
(2) Secretary of the Navy
(3) Secretary of the Air Force
(4) Vice Chairman of the Joint Chiefs of Staff
(5) Under Secretary of Defense for Acquisition and Sustainment
(6) Under Secretary of Defense for Research and Engineering,
(7) Under Secretary of Defense for Policy
(8) DoD Chief Information Officer
(9) Under Secretary of Defense for Intelligence and Security
(10) Director, National Security Agency/Chief, Central Security Service
(11) Commander, United States Space Command
(12) Commander, United States Strategic Command
(13) Commander, United States Northern Command
(14) Commander, United States Cyber Command.

Non-voting Participants:
(1) Under Secretary of Defense (Comptroller)/Chief Financial Officer
(2) Director of Operational Test and Evaluation
(3) Director, National Geospatial-Intelligence Agency
(4) Director, National Reconnaissance Office
(5) Director of Cost Assessment and Program Evaluation.

Figure 1. DoD PNT Enterprise Oversight Governance Process



SecDef – Secretary of Defense
Dep SecDef – Deputy Secretary of Defense
USD(R&E) – Under Secretary of Defense for Research and Engineering
USD(A&S) – Under Secretary of Defense for Acquisition and Sustainment
VCJCS – Vice Chairman of the Joint Chiefs of Staff
DoD CIO – DoD Chief Information Officer

DoDD 4650.05, June 9, 2016
Change 3, April 25, 2023

Figure 6 – DoD PNT Enterprise Governance Process

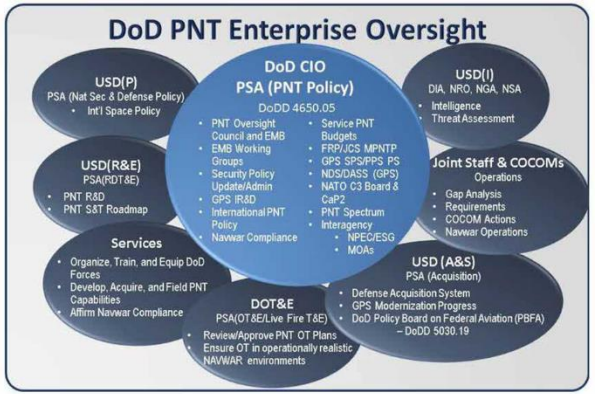


Figure 5 – DoD PNT Enterprise Authorities

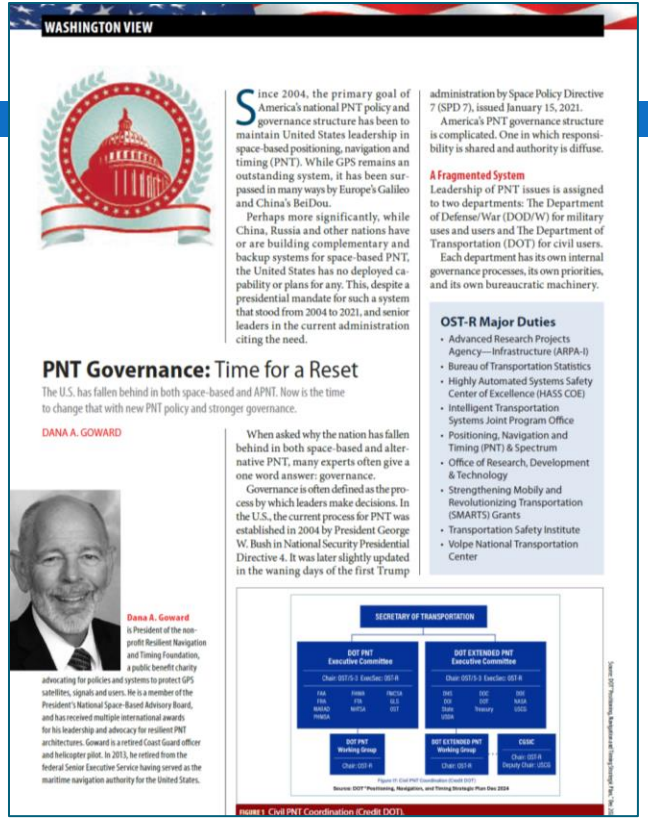
Structure/ process

Space-based only

Everyone & no one responsible

Too many players

No top-down mandate



WASHINGTON VIEW

Since 2004, the primary goal of America's national PNT policy and governance structure has been to maintain United States leadership in space-based positioning, navigation and timing (PNT). While GPS remains an outstanding system, it has been surpassed in many ways by Europe's Galileo and China's BeiDou.

Perhaps more significantly, while China, Russia and other nations have or are building complementary and backup systems for space-based PNT, the United States has no deployed capability or plans for any. This, despite a presidential mandate for such a system that stood from 2004 to 2021, and senior leaders in the current administration citing the need.

administration by Space Policy Directive 7 (SPD 7), issued January 15, 2021.

America's PNT governance structure is complicated. One in which responsibility is shared and authority is diffuse.

A Fragmented System

Leadership of PNT issues is assigned to two departments: The Department of Defense/War (DOD/W) for military uses and users and The Department of Transportation (DOT) for civil users.

Each department has its own internal governance processes, its own priorities, and its own bureaucratic machinery.

OST-R Major Duties

- Advanced Research Projects Agency—Infrastructure (ARPA-I)
- Bureau of Transportation Statistics
- Highly Automated Systems Safety Center of Excellence (HASS COE)
- Intelligent Transportation Systems Joint Program Office
- Positioning, Navigation and Timing (PNT) & Spectrum
- Office of Research, Development & Technology
- Strengthening Mobily and Revolutionizing Transportation (SMARTS) Grants
- Transportation Safety Institute
- Volpe National Transportation Center

PNT Governance: Time for a Reset

The U.S. has fallen behind in both space-based and APNT. Now is the time to change that with new PNT policy and stronger governance.

DANA A. GOWARD

When asked why the nation has fallen behind in both space-based and alternative PNT, many experts often give a one word answer: governance.

Governance is often defined as the process by which leaders make decisions. In the U.S., the current process for PNT was established in 2004 by President George W. Bush in National Security Presidential Directive 4. It was later slightly updated in the waning days of the first Trump

Dana A. Goward is President of the nonprofit Resilient Navigation and Timing Foundation, a public benefit charity advocating for policies and systems to protect GPS satellites, signals and users. He is a member of the President's National Space-Based Advisory Board, and has received multiple international awards for his leadership and advocacy for resilient PNT architectures. Goward is a retired Coast Guard officer and helicopter pilot. In 2013, he retired from the federal Senior Executive Service having served as the maritime navigation authority for the United States.

FIGURE 1 Civil PNT Coordination (Credit DOT).

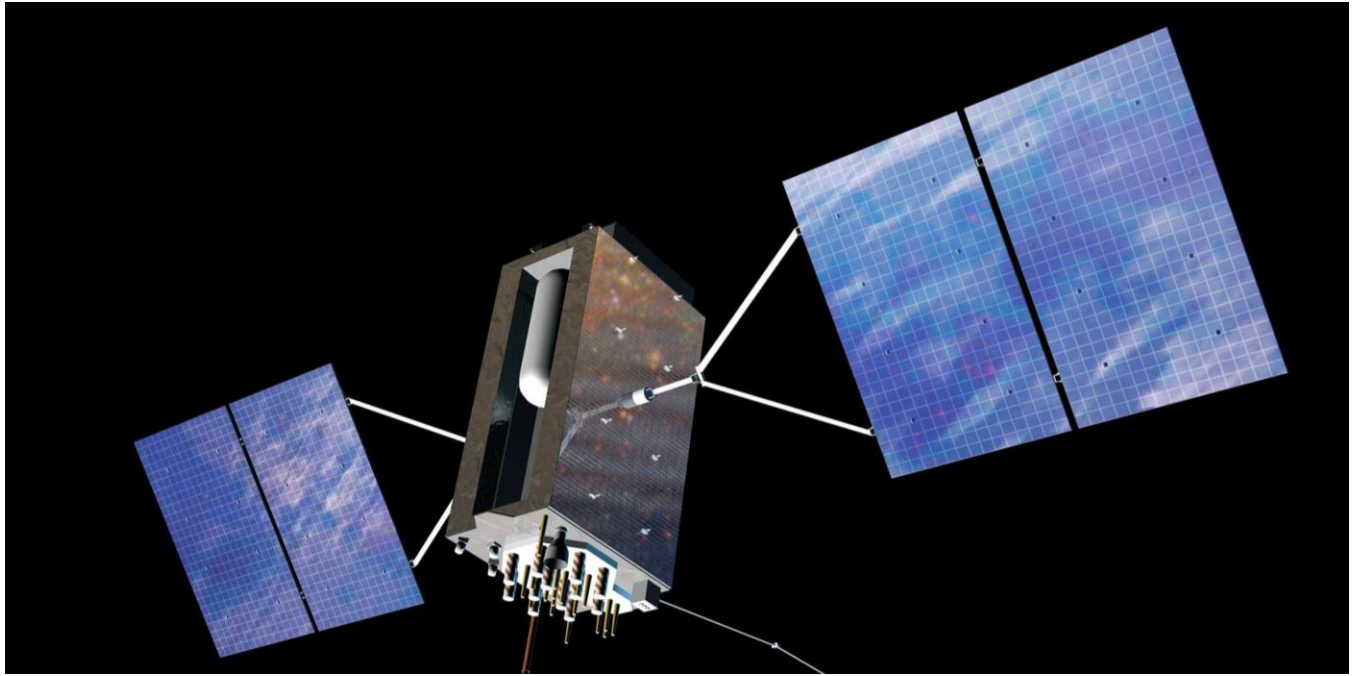
Inside GNSS+ March/April 2026

7 Policy Myths

1. GNSS is enough.

7 Policy Myths

2. “We have to (or ‘they want to’) replace GNSS.”



7 Policy Myths

3. More study is needed.

7 Policy Myths

4. “It’s all about infrastructure protection.”

7 Policy Myths

5. “We just need to educate users.”

7 Policy Myths

6. "The government needs to build a GNSS backup system."

7 Policy Myths

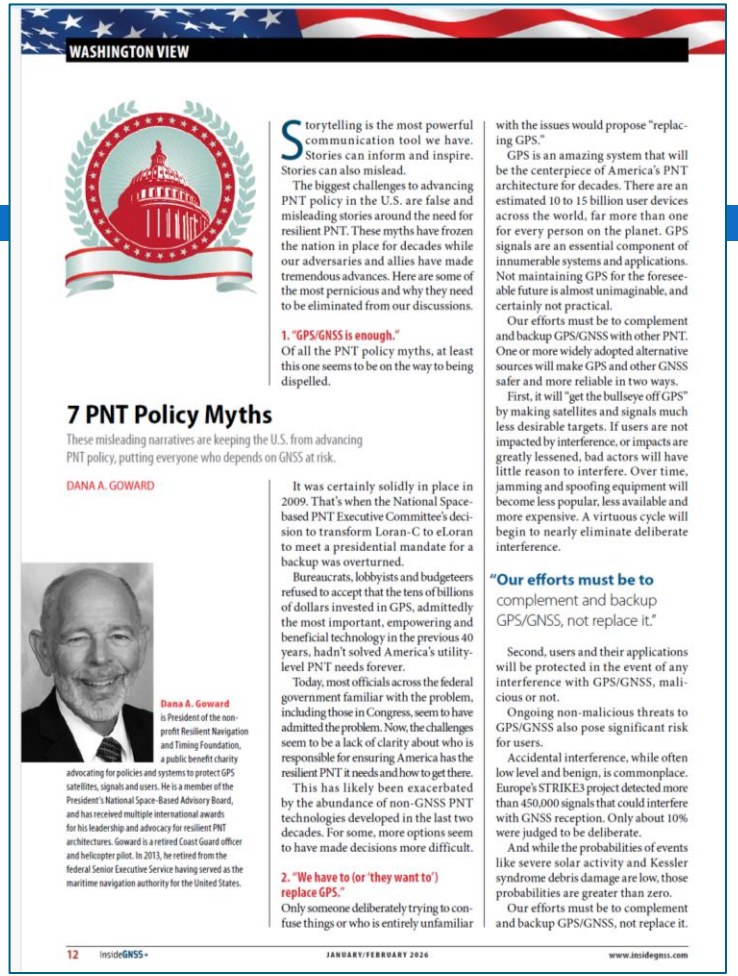
7. "The market will provide the GNSS backup nations need. Governments don't need to do anything."

7 Policy Myths

People = 90% Emotion + 10% Logic

People act after:

- Bad things happen
- Emotionally impactful stories to
  - Avoid bad things
  - Obtain good things



WASHINGTON VIEW

7 PNT Policy Myths

These misleading narratives are keeping the U.S. from advancing PNT policy, putting everyone who depends on GNSS at risk.

DANA A. GOWARD

Dana A. Goward is President of the non-profit Resilient Navigation and Timing Foundation, a public benefit charity advocating for policies and systems to protect GPS satellites, signals and users. He is a member of the President's National Space-Based Advisory Board, and has received multiple international awards for his leadership and advocacy for resilient PNT architectures. Goward is a retired Coast Guard officer and helicopter pilot. In 2013, he retired from the federal Senior Executive Service having served as the maritime navigation authority for the United States.

Storytelling is the most powerful communication tool we have. Stories can inform and inspire. Stories can also mislead.

The biggest challenges to advancing PNT policy in the U.S. are false and misleading stories around the need for resilient PNT. These myths have frozen the nation in place for decades while our adversaries and allies have made tremendous advances. Here are some of the most pernicious and why they need to be eliminated from our discussions.

1. "GPS/GNSS is enough."

Of all the PNT policy myths, at least this one seems to be on the way to being dispelled.

It was certainly solidly in place in 2009. That's when the National Space-based PNT Executive Committee's decision to transform Loran-C to eLoran to meet a presidential mandate for a backup was overturned.

Bureaucrats, lobbyists and budgeteers refused to accept that the tens of billions of dollars invested in GPS, admittedly the most important, empowering and beneficial technology in the previous 40 years, hadn't solved America's utility-level PNT needs forever.

Today, most officials across the federal government familiar with the problem, including those in Congress, seem to have admitted the problem. Now, the challenges seem to be a lack of clarity about who is responsible for ensuring America has the resilient PNT it needs and how to get there.

This has likely been exacerbated by the abundance of non-GNSS PNT technologies developed in the last two decades. For some, more options seem to have made decisions more difficult.

2. "We have to (or 'they want to') replace GPS."

Only someone deliberately trying to confuse things or who is entirely unfamiliar with the issues would propose "replacing GPS."

GPS is an amazing system that will be the centerpiece of America's PNT architecture for decades. There are an estimated 10 to 15 billion user devices across the world, far more than one for every person on the planet. GPS signals are an essential component of innumerable systems and applications. Not maintaining GPS for the foreseeable future is almost unimaginable, and certainly not practical.

Our efforts must be to complement and backup GPS/GNSS with other PNT. One or more widely adopted alternative sources will make GPS and other GNSS safer and more reliable in two ways.

First, it will "get the bullseye off GPS" by making satellites and signals much less desirable targets. If users are not impacted by interference, or impacts are greatly lessened, bad actors will have little reason to interfere. Over time, jamming and spoofing equipment will become less popular, less available and more expensive. A virtuous cycle will begin to nearly eliminate deliberate interference.

"Our efforts must be to complement and backup GPS/GNSS, not replace it."

Second, users and their applications will be protected in the event of any interference with GPS/GNSS, malicious or not.

Ongoing non-malicious threats to GPS/GNSS also pose significant risk for users.

Accidental interference, while often low level and benign, is commonplace. Europe's STRIKE3 project detected more than 450,000 signals that could interfere with GNSS reception. Only about 10% were judged to be deliberate.

And while the probabilities of events like severe solar activity and Kessler syndrome debris damage are low, those probabilities are greater than zero.

Our efforts must be to complement and backup GPS/GNSS, not replace it.

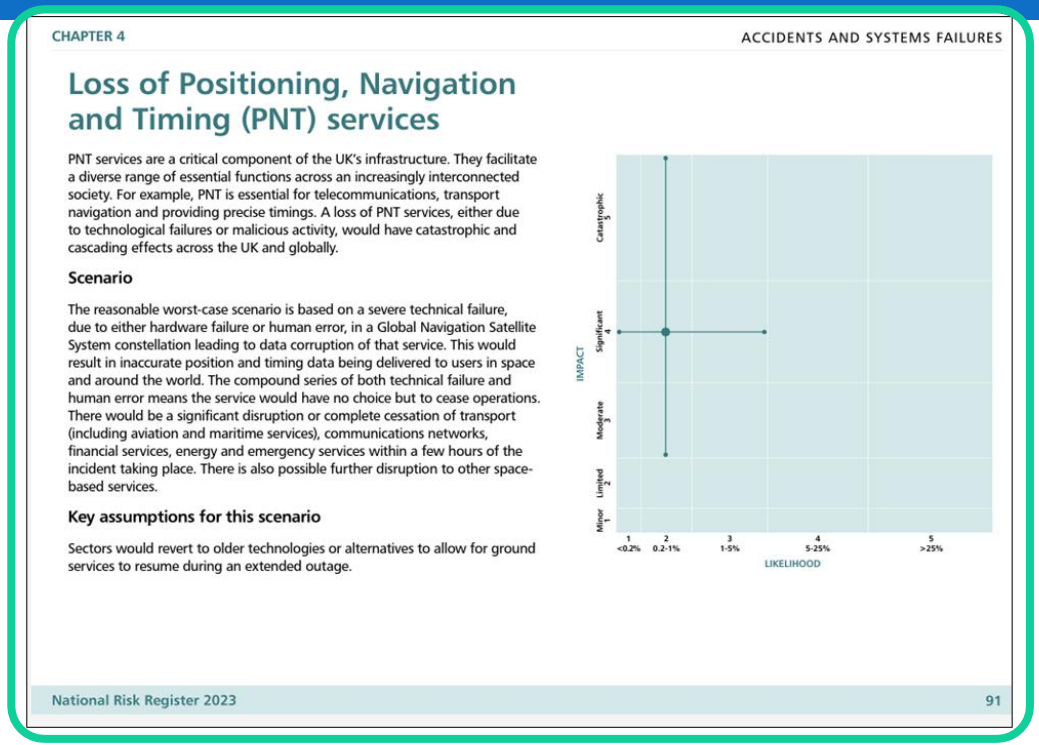
Inside GNSS+ Jan/Feb 2026

UK Showing the way

A NATIONAL PNT RISK

Department for Science, Innovation & Technology

- Assessed that **97% of UK CNI was dependent on GNSS services**
- **90% of users relied on GPS**
- **Risks to GNSS include:**
  - Loss due to system failure
  - Loss due to hostile act
  - Loss due to space weather
- Economic Impact of 1 week's disruption - **£7.4bn** ($9.6bn/€8.8bn)



CHAPTER 4 ACCIDENTS AND SYSTEMS FAILURES

Loss of Positioning, Navigation and Timing (PNT) services

PNT services are a critical component of the UK's infrastructure. They facilitate a diverse range of essential functions across an increasingly interconnected society. For example, PNT is essential for telecommunications, transport navigation and providing precise timings. A loss of PNT services, either due to technological failures or malicious activity, would have catastrophic and cascading effects across the UK and globally.

Scenario

The reasonable worst-case scenario is based on a severe technical failure, due to either hardware failure or human error, in a Global Navigation Satellite System constellation leading to data corruption of that service. This would result in inaccurate position and timing data being delivered to users in space and around the world. The compound series of both technical failure and human error means the service would have no choice but to cease operations. There would be a significant disruption or complete cessation of transport (including aviation and maritime services), communications networks, financial services, energy and emergency services within a few hours of the incident taking place. There is also possible further disruption to other space-based services.

Key assumptions for this scenario

Sectors would revert to older technologies or alternatives to allow for ground services to resume during an extended outage.

National Risk Register 2023 91

https://www.gov.uk/government/publications/national-risk-register-2025

Risk of Loss of PNT – More Than One Cause

Department for Science, Innovation & Technology

UK National Risks to Positioning, Navigation & Timing

Severe Space Weather
Solar flares and geomagnetic storms disrupt GNSS signals
Wide-area degradation

Hostile Acts
Jamming, spoofing and cyber attacks
Intentional disruption of GNSS

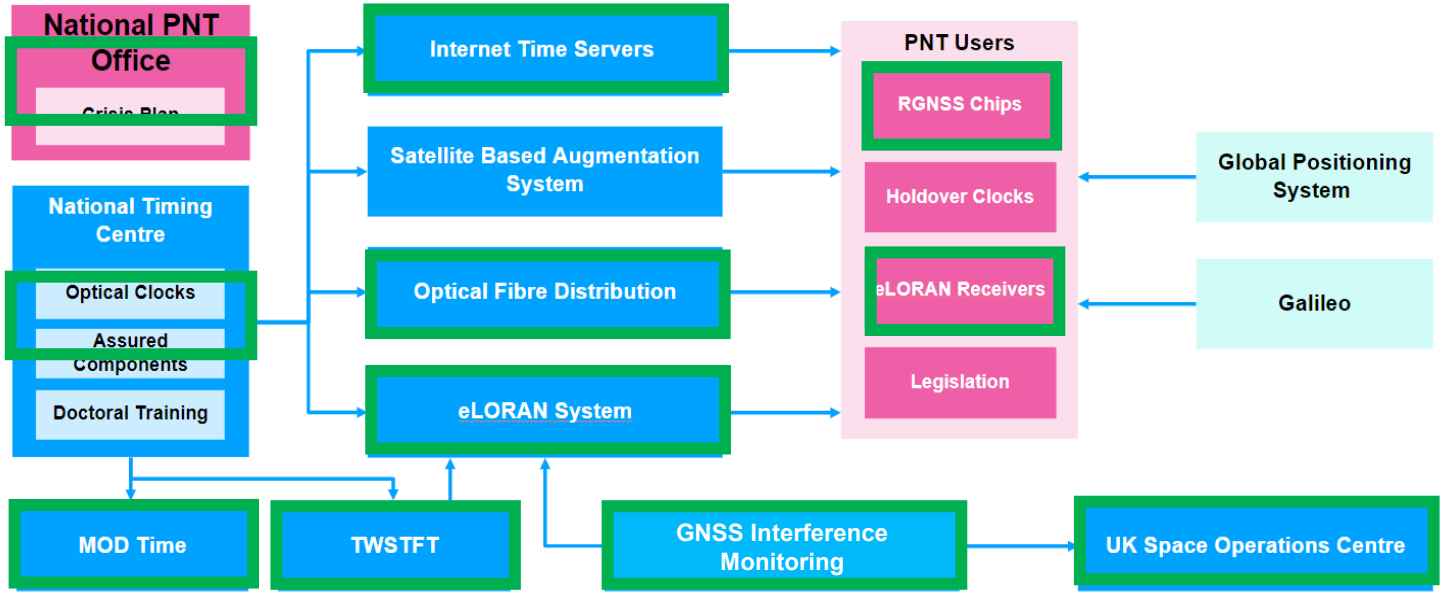
Failure of PNT Systems
Satellite or ground failures
Systemic dependency risks

National Impact

Telecommunications networks
Financial systems & trading
Energy grid synchronisation
Aviation & maritime navigation
Autonomous systems & logistics

Delivery Progress:

Department for Science, Innovation & Technology



100% of funding approved by UK Treasury for National PNT initiatives – £450m+ for 2025-2030 delivery

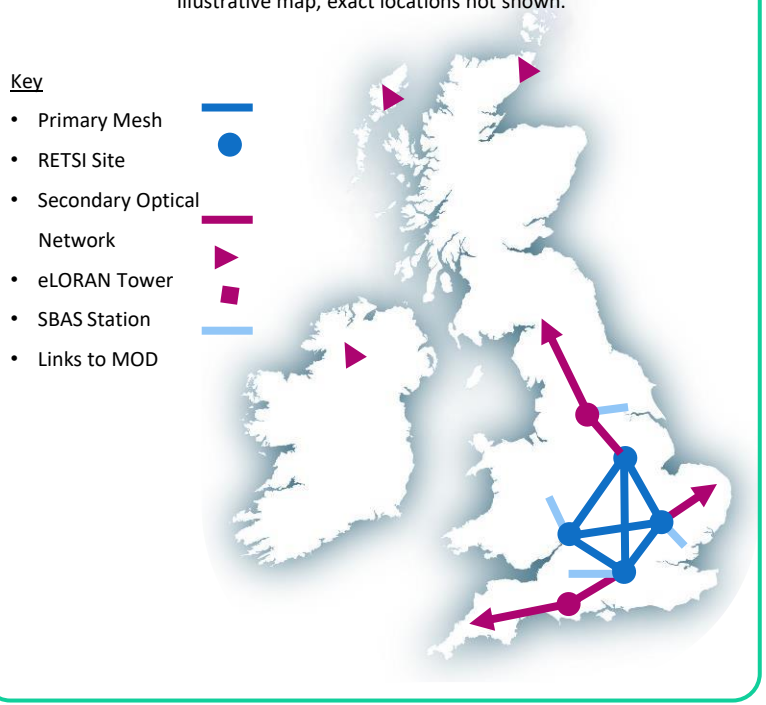
TIMING DISTRIBUTION

Department for Science, Innovation & Technology

- The Policy Framework commits to developing separate business case proposals for an **Enhanced Long-Range Navigation (eLORAN)** system and a **Space Based Augmentation System (SBAS)** and working with MOD on **Defence Resilient Time (DRT)**.
- A Secondary Fibre Optic Cables Network would provide the Timing Signal from the RETSI sites to the eLORAN towers, Goonhilly Station for SBAS, and locations for DRT.
- The Secondary Fibre Optic Cables Network would consist of 11 Service Nodes, including: 4 at RETSI sites, 3 at eLORAN towers, 2 intermediate nodes, 1 MOD private node and 1 at an SBAS station.

Map of the Primary Mesh and Secondary Fibre Optic Cables Network

Illustrative map, exact locations not shown.

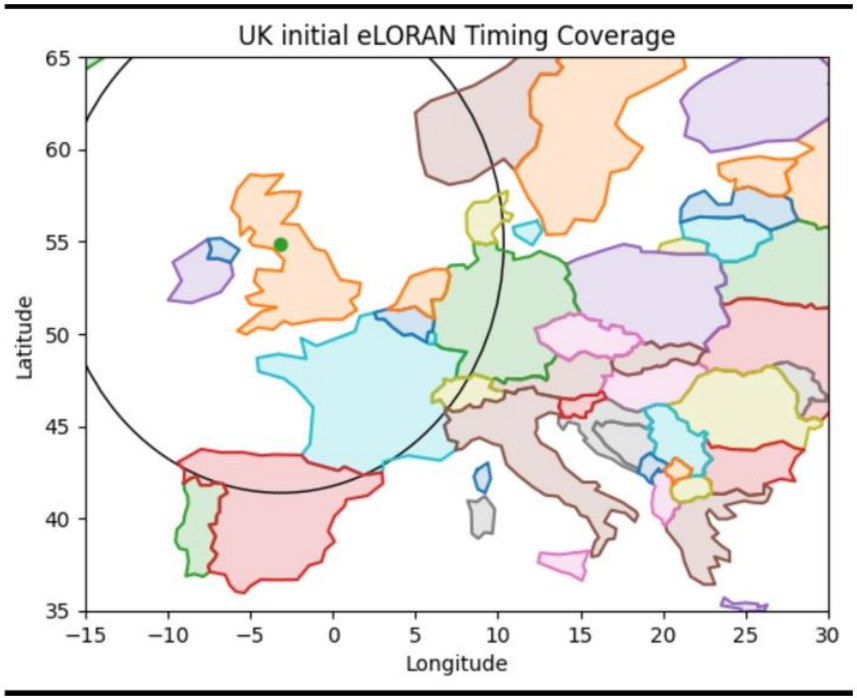


UK National eLORAN for Timing Services

Department for Science, Innovation & Technology

UK eLORAN Chain Coverage – Timing

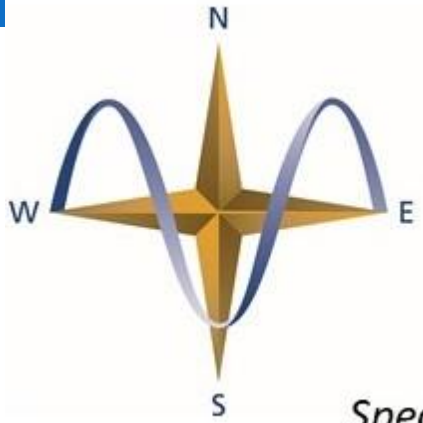
- IOC Jan 2027
- 20 nanosecond target
- Available underwater and up to 85 metres underground
- UTC (NPL) primary timescale
- UTC (OP) as secondary
- MOD Timescale of last resort



International eLORAN Conference - Mar 2026

Department for Science, Innovation & Technology

14 Nations, 4 Continents, EU, IALA, ESA and IMO



RESILIENT NAVIGATION *and* TIMING FOUNDATION

Speaking Up for GPS/GNSS Users

The Resilient Navigation and Timing Foundation is a 501(c)3 educational and scientific charity registered in Virginia

www.RNTFnd.org