FRONTIER SI

AUSTRALIA'S NAVIGATION AND TIMING CHALLENGES ON HAZARDS, OPERATIONS, AND RESILIENCE (ANCHOR)

FEBRUARY 2026

ACKNOWLEDGEMENT

FrontierSI respectfully acknowledges the Aboriginal and Torres Strait Islander people of Australia, first custodians of the lands, air and waters that sustain the places we live, work and play. These first peoples have had a vibrant, living culture that has remained in sustainable synergy with the natural environment for tens of thousands of years, and continue to do so.

We recognise that the lands of the Aboriginal and Torres Strait Islander people of Australia coexist with the Commonwealth of Australia.

This report is part of the project "Armouring the Clock: Providing Direction to Resilient Positioning, Navigation, and Timing (PNT)", funded under the 2024 Department of Defence Strategic Policy Grants Program.

The authors of this report are:

- Eldar Rubinov (FrontierSI)
- Jia Lee (FrontierSI)
- Joshua Critchley-Marrows (Independent Consultant)

Valuable feedback was received from Dana Goward (Resilient Navigation and Timing Foundation), Andy Proctor (RethinkPNT) and James Leversha (FrontierSI).

CREATIVE COMMONS LICENSE

Citation

FrontierSI (2026), Australia's Navigation and Timing Challenges on Hazards, Operations and Resilience (ANCHOR), available at frontiersi.com.au.

AI DISCLOSURE STATEMENT

FrontierSI has utilised Artificial Intelligence (AI) to generate initial drafts and brainstorm content in the production of this work. FrontierSI uses ChatGPT, GitHub CoPilot, Microsoft CoPilot and their associated models. FrontierSI always carefully scrutinises, modifies and expands upon AI-generated content to ensure accuracy and original authorship. FrontierSI will never distribute work that is purely AI-generated.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

Acronym	Full form
3GPP	3rd Generation Partnership Project
ADF	Australian Defence Force
ADS-B	Automatic Dependent Surveillance-Broadcast
AGC	Automatic Gain Control
AIS	Automatic identification System
ALIS	Anchored Location Integrity System
AOIP	Area of Interest Prediction
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
ASAT	Anti-Satellite
ASF	Additional Secondary Factor
ATC	Air Traffic Control
BPS	Broadcast Positioning System
C5ISR	Command Control Communications Computers Cyber Intelligence Surveillance and Reconnaissance
CDMA	Code Division Multiple Access
CEMA	Cyber and Electromagnetic Activities
CHIMERA	Chips Message Robust Authentication
CISC	Critical Infrastructure Security Centre
CORS	Continuously Operating Reference Station
CRPA	Controlled Reception Pattern Antenna
CSAC	Chip-Scale Atomic Clock
CSIS	Center for Strategic and International Studies
DTG	Dynamically Tuned Gyroscope
EAR	Export Administration Regulations
EGNOS	European Geostationary Navigation Overlay Service
ESA	European Space Agency
EW	Electronic Warfare
FAA	Federal Aviation Administration
FCC	Federal Communication Commission
FDMA	Frequency Division Multiple Access
FOG	Fibre-Optic Gyroscope
GBAS	Ground Based Augmentation System
GEO	Geostationary Orbit
GNSS	Global Navigational Satellite Systems
GPS	Global Positioning System
ICAO	International Civil Aviation Organisation
ICG	International Committee on GNSS
IDPS	Independently Derived Positioning System
INS	Inertial Navigation System

Acronym	Full form
IoD	In-orbit-Demonstration
ITAR	International Traffic in Arms Regulations
ITU	International Telecommunications Union
KPS	Korean Positioning System
LEO	Low Earth Orbit
LPV	Localiser Performance with Vertical guidance
MarRINav	Maritime Resilience and Integrity in Navigation
MEMS	Micro-Electro-Mechanical Systems
MEO	Medium Earth Orbit
NavIC	Navigating with Indian Constellation
NIC	Navigation Integrity Category
NMR	Nuclear Magnetic Resonance
NOTAM	Notice to Airmen
NTN	Non-Terrestrial Network
NTP	Network Time Protocol
NTS-3	Navigation Technology Satellite-3
NV	Nitrogen-Vacancy
OCXO	Oven-Controlled Crystal Oscillator
OPM	Optically Pumped Magnetometer
OpSTAR	Optical Synchronised Time and Ranging
OSNMA	Open Service Navigation Message Authentication
PNT	Positioning Navigation and Timing
PNT-SA	Positioning Navigation and Timing Situational Awareness
PTP	Precision Time Protocol
QZSS	Quasi-Zenith Satellite System
RAIM	Receiver Autonomous Integrity Monitoring
RFI	Radio Frequency Interference
R-GPS	Resilient GPS
RLG	Ring Laser Gyroscope
SCADA	Supervisory Control And Data Acquisition
SoOP	Signals of Opportunity
SQUID	Superconducting Quantum Interference Device
TCXO	Temperature-Compensated Crystal Oscillator
TWSTFT	Two-Way Satellite Time and Frequency Transfer
SBAS	Satellite Based Augmentation System
SoL	Safety-of-Life
USML	United States Munitions List
VDES	VHF Data Exchange System
WAAS	Wide Area Augmentation System

EXECUTIVE SUMMARY

FrontierSI's ANCHOR report is intended for Defence and Australian Government policy and decision makers, critical infrastructure sector leaders and operators, engineers, and the global positioning, navigation, and timing (PNT) community. The report is organised into two parts.

Part I establishes a common language framework to understand Australia's PNT threat environment, evaluating threats through both a civil government hazards-based lens, as well as from a military framework of cooperation, competition, and conflict. This offers a rationale and supporting examples for recognising PNT threats that extend well beyond radiofrequency interference.

Part II focuses on strengthening Australia's PNT resilience. It begins with PNT situational awareness from a radiofrequency interference perspective as the most observable PNT threat area, then examines a comprehensive range of available PNT technologies. Finally it synthesises architectural options that could be further explored to address different threats.

Australia's PNT posture is increasingly exposed to disruption

A threat to Australia's PNT goes far beyond impacts to technical systems or isolated services, as even small disruptions can have cascading consequences, creating risks to national and economic security. Australia's primary reliance on GPS can lead to critical points of failure, limited control over timing services, and potential supply chain choke points. Essentially, Australia's PNT posture lacks the diversity, redundancy, resilience to manage contemporary threats that are both emerging and that can be layered across a continuum of strategic conditions (cooperation, competition, conflict). Adversaries could view Australia's lack of PNT signal diversity as an opportunity to create disruption. Indeed, disruptions to PNT have become a routine modus operandi in the grey-zone state, and these only escalate and amplify during conflict.

Fragmented PNT responsibility undermines threat recognition and response

Responsibility for PNT in Australia remains fragmented, with both overlapping roles and gaps across government and industry. This fragmentation weakens Australia's ability to recognise and respond to PNT threats, and therefore hinders the coordination of timely and effective deterrence and response measures. PNT threats are often associated with deliberate interference events, such as jamming and spoofing. However, there are a broader range of physical, natural, cyber and information, supply chain, and personnel hazards that are not readily recognised as PNT threats, despite their potential to degrade the availability, integrity and trustworthiness of PNT services.

A shared civil-military framework is essential for managing PNT threats

A common language is required to articulate how threats to PNT might be jointly recognised from both civil (such as the Australian Department of Home Affairs) and military (Australian Department of Defence) perspectives. In aligning threats with both hazard classes and the cooperation-competition-conflict spectrum, it enables a broad range of stakeholders to assess how threats could manifest and evolve across strategic environments. Finally, this shared civil-military framework provides options for how strategic PNT architectures could help deter the threat and/or mitigate the risk of impact as part of Australia's position in the Indo-Pacific region. Importantly this work provides a foundation for future coordinated efforts at the national-scale to detect, respond, and anticipate threats to PNT in an integrated manner.

Threat and Resilience Levers: Key Findings

1. **PNT threats** can manifest either individually or in parallel across the cooperation-competition-conflict framework that reflects the full continuum from peacetime interaction through to conflict. Each threat has a potential to be a force multiplier, including an adversary leveraging natural disasters to gain technical or soft power advantage.
2. **PNT resilience levers** need to be combined and emphasised to address different hazard classes. The responsibility of activating the levers of System, Governance, Policy, and enabling Technology can be allocated to the appropriate functions across Defence and civil government in which to achieve a more resilient PNT posture.
3. **Cyber, information and electromagnetic**-related hazards represent a prominent subset of PNT threats and often occur below the threshold of conflict. While some incidents may be difficult to attribute to particular actors, they can still have a significant operational impact on PNT services. The threats can be deterred through cyber and EM-hardening of systems, and potential impacts can be mitigated through access to portable, scalable PNT alternatives.
4. **Physical and kinetic** threats increase sharply in crisis and war. Australia is not presently within what defines traditional kinetic warfare on home soil. However forward-looking deterrence and mitigation can be achieved via the establishment of multi-layered PNT infrastructure and services either in space and/or terrestrially, and having mechanisms in place for coordinated response.
5. **Supply chain** vulnerabilities are increasingly exploited in competition, and this is exacerbated by Australia's lack of self-sufficiency in developing core PNT componentry and systems. Deterrence could be achieved by securing access to these elements through strong trade partnerships, and establishing industrial policies that support domestic manufacturing of critical components.

6. **Personnel-related** PNT threats can be used to initiate and layer on other threats. Robust organisational and governance mechanisms are needed as the first layer of deterrence. Additionally establishing distributed PNT architectures and systems is a logical approach to mitigating the risk of these threats, whether intentional or unintentional.
7. **Natural hazards** impose baseline moderate to severe consequences across the competition spectrum should they occur. Whilst they cannot be deterred, their impacts on PNT can be mitigated through redundancy and diversity in GNSS and PNT sources.
8. **A threat-driven approach** to PNT resilience can help inform future risk and consequence. It can also provide a guiding framework for decisions on a multi-layered PNT approach for Australia.

Resilient PNT as a System-Level Challenge

A wide range of resilient PNT technologies is currently being developed across space-based systems, terrestrial broadcasts, and onboard sensors, including emerging quantum capabilities. These technologies span varying levels of maturity, from fully operational to an early stage of development, but are progressing rapidly.

However, resilient PNT should not be framed as a problem that can be solved through the procurement of a single technology or platform. The diversity of available and emerging options makes it unclear which technologies should be prioritised. Rigorous validation, testing, and operational assessment is needed to understand the pros and cons of each technology and how it is suited for Australia.

More fundamentally, technology alone does not deliver resilience. Resilience is determined by how PNT systems behave over time. This involves how threats are detected, how systems (both human and and technical) respond, how performance degrades, and how quickly and reliably recovery occurs. Once this is understood, technology choices can be made in a targeted and outcome-driven manner.

Multi-Layered PNT Approach: Key Findings

1. **Space-based technologies** including GNSS, Satellite Based Augmentation Systems (SBAS), Low Earth Orbit (LEO) PNT systems, hybrid multi-orbit architectures, and the VHF Data Exchange System (VDES) provide wide-area PNT coverage and remain the primary source of absolute PNT for most civil and defence users, while multi-orbit and augmentation approaches can improve availability, performance, and resilience.
2. **Terrestrial broadcast technologies** such as eLoran, Ranging Mode (R-Mode), pseudolite networks, 5G broadcast, as well as television and radio signals provide terrestrially sourced PNT that is physically and operationally independent of GNSS, offering complementary coverage and enhanced resilience in contested or degraded environments.
3. **Time transfer, synchronisation, and holdover** enable the distribution of precise and resilient time across Defence networks and critical infrastructures, as well as sustaining operations during GNSS disruptions.
4. **Onboard sensors** including inertial navigation systems (INS), magnetic anomaly-aided navigation (MagNav), gravity anomaly-aided navigation (GravNav), and environmental or context-based sensors support navigation in GNSS-denied environments by exploiting locally available signals or physical phenomena, with both classical and emerging quantum technologies offering complementary performance trade-offs.
5. **Artificial intelligence (AI) and machine learning (ML)** act as cross-cutting enablers for resilient PNT by improving detection of anomalies, interference, and deception, and by supporting sensor fusion and adaptive system behaviour. AI/ML does not replace deterministic PNT, but enhances resilience when applied in bounded, explainable roles and integrated within multi-layer architectures, reinforcing the need for strong governance and assurance.

Recommendations

ANCHOR makes the following recommendations:

1. **Define nationally-coordinated threat-driven and risk-based requirements for PNT resilience.**
   Establish clear, nationally-consistent requirements that specify the level of PNT resilience needed to maintain essential services and national security functions. These requirements should be based on identified PNT threats, and both civil and Defence operational outcomes.
2. **Undertake feasibility studies of PNT architectures to meet these requirements.**
   Evaluate a range of complementary and layered PNT architectures to determine their technical feasibility, cost, scalability, and ability to meet both civil and Defence PNT resilience requirements.
3. **Review existing policy, regulatory, and standards frameworks to support resilient PNT outcomes.**
   Assess how current policies, regulations and standards governing critical infrastructure sectors can be leveraged, adapted, or amended to accelerate adoption of resilient PNT architectures and best-practices. Ensure these frameworks also support Defence assurance and interoperability requirements.
4. **Develop an Australian PNT Strategy to guide Australia's future PNT capability.**
   Create a whole-of-nation PNT Strategy that provides strategic direction for Australia's future PNT capability. The Strategy should clarify roles and responsibilities across Defence, civil agencies, and industry, and align stakeholders towards a coordinated resilient PNT capability for Australia. The Strategy should also make steps towards outlining implementation roadmaps and regulatory instruments, such as a Radio Navigation Plan.

1 INTRODUCTION

1.1 Increased Threat Tempo and Move Towards Resilience

The global Positioning, Navigation, and Timing (PNT) environment is changing faster now than at any point since the inception of Global Navigation Satellite Systems (GNSS). What was once a system that exponentially opened up opportunities for national security, technological acceleration, and economic development, PNT is now a tool leveraged for competition, interference, and space power. GNSS disruptions were once rare events, but now they occur daily across multiple regions including Australia.

Globally there has been a sharp rise in instances of deliberate interference with GNSS signals in military exercises, grey-zone activities, and regional conflicts. Technological barriers are also falling, with low-cost interference kits, cyber capabilities, and artificial intelligence being easily accessible to non-state actors. In parallel, space is becoming more congested and contested, increasing the risk of satellite failure or hostile action.

Threats to PNT arise in many forms. Some are overt, such as jamming and spoofing, and others are more subtle, such as software errors, supply chain compromise, failures in PNT-dependent critical infrastructure. The availability and integrity of PNT information can also be impacted by faulty electrical equipment, misconfigured transmitters, or other inadvertent emissions, which, although unintentional, can nonetheless produce operationally-significant PNT disruptions. Many of these vulnerabilities are not immediately recognised as threats to PNT, yet the consequences felt across national coordination and Defence operations could be traced back to how these threats affect the availability and integrity of PNT information. Collectively, these conditions have quietly shifted PNT's status from an *invisible utility* to an area of strategic competition, exposed to a broad range of hazard types.

Several nations, such as United States, United Kingdom, European Union, Japan, China, and South Korea amongst others, have responded to this increased risk by elevating PNT resilience to a national priority. These countries are investing in national PNT policy and governance frameworks to inform infrastructure and situational awareness capabilities, as well as multi-layered approaches that combine satellite services (e.g., GNSS, regional augmentation, LEO PNT), terrestrial broadcast technologies (e.g., eLoran, R-mode), GNSS-independent timing backbones, and complementary sensor technologies (e.g., inertial, quantum, visual). As a result, PNT resilience can be seen as being developed through diversity, redundancy, monitoring, and adaptive response across the full PNT ecosystem, rather than through any single technology solution alone [1].

Australia's reliance on GNSS is particularly acute due to the country's geographic scale, dispersed population, and dependence on long-range transport and remote operations. Australia depends heavily on the US Global Positioning System (GPS) to enable national infrastructure, military operations, and daily functioning of the economy. Even Australia's SouthPAN satellite-based augmentation system (SBAS) relies on GPS data as essential input. Disruptions to PNT can therefore cascade across sectors including aviation, maritime, telecommunications, energy and finance.

The dialogue about PNT disruptions and implications for Defence operations and civilian critical infrastructure is becoming more mainstream. However, at this point Australia has not formalised a national PNT strategy or policy. Beyond this need for strategic leadership, the main challenge is ensuring and maintaining awareness of threats to PNT, and treating them as systemic challenges. The Australian government requires strategic planning to recognise PNT threats in its many forms, rather than viewing PNT threats as isolated technical events impacting individual sectors or users.

FrontierSI's ANCHOR report examines the shift of PNT from an enabler to an enabler-at-risk. It looks at threats to PNT across multiple hazard types, from jamming and spoofing to supply chain and personnel hazards. It considers the threat consequence from both military (Defence) and civilian (Home Affairs) angles, and evaluates how the PNT threats evolve across the cooperation-competition-conflict spectrum. While previous FrontierSI work has focused on recommendations for PNT governance in Australia, this report places particular emphasis on threat recognition and framing, before reviewing technology capabilities and presenting options for multi-layered technology architecture.

ANCHOR aligns with emerging international efforts, including the UK Space Agency's freshly released SPARK publication, which focuses on PNT situational awareness and technology domains [2]. ANCHOR complements this by establishing a shared civil-military understanding of the PNT threat environment to inform technology, architectural, and policy choices.

This is the third report as part of FrontierSI's "Armouring the Clock" project funded through the Defence Strategic Policy Grants Program. The first report assessed the PNT disruptions and their impacts on defence [3], and the second report examined international PNT policies and governance models that could be adapted to Australia [4].

1.2 Report Purpose and Scope

This report assesses the current and emerging PNT threat environment, contextualised for Australia's policy and strategic interests, industrial landscape, and operational needs. The objectives are to:

- Characterise the contemporary PNT threat landscape against hazard types as applied to Australia's critical infrastructure.
- Evaluate Australia's exposure to PNT threats through a military and civilian security lens.
- Outline the global trends in PNT technologies and architectures.
- Consider PNT architectures that Australia could consider to mitigate PNT threats.

The following sections are set out:

- **Chapter 1** (this chapter) sets the context for how Australia uses PNT and the threats that challenge PNT continuity, integrity and resilience.
- **Part I: Understanding Australia's PNT Threat Environment**
  - **Chapter 2** examines the PNT threat landscape through a technical and operational lens, mapping threats across the hazard types of physical, natural, supply chain, personnel, and cyber-information-electromagnetic.
  - **Chapter 3** assesses Australia's exposure to PNT vulnerabilities across the spectrum of peace, grey zone, and war, and highlights implications for Defence and Home Affairs, who approach PNT from different operational and policy perspectives.
- **Part II: Strengthening Australia's PNT Resilience**
  - **Chapter 4** examines the ways to detect and respond to PNT threats as an operational and decision-support capability, concentrating mainly on radiofrequency (RF) threats, as they represent the most immediate hazard in the current operational environment.
  - **Chapter 5** identifies and assesses key technologies being adopted or trialled globally to enhance PNT resilience, considering their roles in multi-layered architectures.
  - **Chapter 6** outlines strategic technology and architectural considerations to support informed decision-making on how Australia can build a more robust, multi-layered, and sovereign PNT capability.
- **Chapter 7** synthesises the findings of a hazard-driven and threat-driven approach to PNT resilience.

PART I: UNDERSTANDING AUSTRALIA'S PNT THREAT ENVIRONMENT

2 CLASSIFICATION OF PNT THREATS

While radiofrequency interference, such as jamming and spoofing, is commonly recognised as a threat to PNT, threats can also arise in less obvious forms. Many are not immediately identified as PNT issues, instead appearing as industrial, economic, or geopolitical challenges. However, these events can impact on the availability and integrity of PNT information. When this information is compromised, it can in turn affect a wide range of operational, assurance, and safety functions across entire sectors.

In this report, PNT threats are first examined through a hazards-based approach, aligned with how the Australian government considers and manages material risks. Applying this framework helps translate abstract or highly technical PNT threats into hazard vector categories that government, critical infrastructure, and Defence operations can readily understand and assess. The Critical Infrastructure Security Centre (CISC) at the Department of Home Affairs defines the following classes of hazards [5] relevant to Australian critical infrastructure entities:

- Cyber and information security hazards
- Physical security hazards
- Natural hazards
- Personnel hazards
- Supply chain hazards

These hazard classes illustrate that disruption to PNT services can arise from a range of sources, including intentional attack, system failure, supply chain weakness, or natural phenomena, often with similar operational consequences. For clarity, the terms hazards and threats are differentiated. Hazard classes are used as the overarching taxonomy, while threats are treated as PNT-specific manifestations of those hazards. For the purposes of this report, Electro-Magnetic (EM) threats will be covered as an extension of cyber-related hazards, consistent with military concepts in cyber and electromagnetic activities (CEMA).

2.1 Cyber, Information, and Electromagnetic Hazards

GNSS and other PNT systems depend on physical assets, digital infrastructure and radiofrequency signals. As such their attack surface extends across cyberspace and the EM spectrum. These two layers are increasingly entangled, as cyber operations can target space and ground-based digital infrastructure, while EM interference can disrupt the signals on which those systems depend. In a 2024 PNT Factsheet for Critical Infrastructure, CISC categorises GNSS jamming and spoofing (as a form of EM interference) under the umbrella of cyber-attacks [6]. This section therefore examines how threats to PNT can be viewed from a cyber, information, and EM hazards lens, rather than as isolated technical failures or intentional RF interference alone.

2.1.1 Cyber Vulnerabilities

While GNSS is often thought of as a purely space-based system, its functionality relies on a complex chain of ground infrastructure, data links, and user equipment. This creates multiple vectors for cyber and information threats that can compromise availability, integrity, and trust in GNSS services.

GNSS receivers are used by systems that depend on PNT data. A 2023 analysis by cybersecurity firm Cyble discovered that thousands of satellite and GNSS receivers from major vendors were exposed to the internet, with many running outdated firmware and/or weak authentication [7]. This sort of exposure significantly expands the attack surface for adversaries seeking opportunities to disrupt or manipulate PNT data. In several cases, hacktivist and cybercrime groups targeted the internet-connected receivers to access, transfer, and/or wipe configuration data on compromised devices. These attacks increasingly demonstrate that remote compromise of GNSS infrastructure is feasible, and that the same access could be used to inject false data, degrade timing accuracy, or disable services that underpin critical systems.

Exposure to cyber risks is magnified when considering that Defence and critical infrastructure sectors are increasingly modernising their digital operations by migrating to distributed cloud-based architectures. While Defence adopts secure and zero trust principles, cyber incidents illustrate that determined actors can still exploit weaknesses that degrade PNT resilience. Intentional or un-intentional compromise of cloud-hosted GNSS management or timing services could have cascading consequences across Defence, telecommunications, power distribution, and financial networks that rely on precise time synchronisation.

Table 1 presents selected cyber incidents that are not specific to PNT, but demonstrate digital vulnerabilities that are directly applicable to understanding threats facing space-enabled PNT services.

Table 1: Examples of cyber incidents relevant to space-enabled or GNSS services.

Example	Year	Type of event	Description	Consequence
Viasat KA-SAT cyber attack	2022	SATCOM ground-network intrusion	Cyber-attack on KA-SAT management segment via a VPN misconfiguration	Loss of satellite broadband service for many users across Europe [8].
GhostSec cyber incident	2023	Hacking of internet-connected GNSS receivers	Malicious updates enabled stealthy access	Compromised devices and unauthorised manipulation of GNSS data [7].

2.1.2 Information Vulnerabilities

Information vulnerabilities affecting PNT services are broadly categorised into information integrity and information availability, reflecting whether incorrect or misleading information is delivered to users, or whether information is unavailable altogether. These sub-categories are described below.

2.1.2.1 Information Integrity

GNSS comprises a highly-networked chain including ground, space, and user segments responsible for generating, distributing, and applying navigation and timing information. Failures within this chain can result in incorrect or misleading PNT data being broadcast while signals remain available to users. These systems can be affected by software configuration or procedural errors, resulting in incorrect or inconsistent PNT information being disseminated to users. Such failures can interfere with the dissemination of ephemeris and clock data, or introduce subtle inconsistencies that degrade the integrity of navigation and timing information without an obvious loss of service. Table 2 presents examples of PNT integrity failures in which incorrect or misleading information was broadcast while services appeared available to users.

Table 2: Examples of PNT integrity failures caused by incorrect or misleading information.

Example	Year	Origin	Consequence
GLONASS Clock Parameter Error	2014	Ground segment (software error)	Incorrect clock data uploaded to multiple satellites [9].
GPS Timing Anomaly	2016	Satellite / system (timing anomaly)	Satellite malfunction caused incorrect GPS timing information to be broadcast globally [10].
Incorrect Nav Messages (GPS)	2025	Satellite software / data fault	Broadcast of faulty navigation data by a single GPS satellite [11].

2.1.2.2 Information Availability

Other than PNT information integrity, information availability failures can arise from a combination of system faults, human or operational error, and deliberate protective actions taken by service providers. Hardware failures, software defects, or maintenance activities within ground or space segments (i.e. supply chain, personnel, or other hazards) can directly disrupt service continuity, while configuration errors or procedural missteps may introduce conditions requiring service withdrawal. In other cases, services are intentionally suspended once anomalies are detected. Whilst this response is based on service assurance, the absence of information availability can nonetheless result in significant loss-of-service impacts for safety-of-life, regulated, and time-critical applications.

The examples in Table 3 relate to SBAS services, which enhance core GNSS capabilities by broadcasting integrity, correction, and availability information via geostationary satellites. SBAS is widely used in safety-critical and regulated applications, particularly aviation, where it enables precision approaches such as Localiser Performance with Vertical guidance (LPV). Because SBAS services are designed to prioritise safety and integrity, detected anomalies often result in conservative service withdrawal rather than continued degraded operation.

Table 3: Examples of GNSS and SBAS availability failures leading to loss of service.

Example	Year	Type of event	Description	Consequence
EGNOS Outage	2012	Ground segment failure	Failure in ground stations caused inconsistent data.	Three day service outage, loss of LPV guidance [12].
Galileo Outage	2019	Ground segment failure	Fault in Precise Timing Facility affected system-wide signal.	Week-long service outage, users reverted to GPS [13].
WAAS Localised Outages	2019	Maintenance, system anomalies	Temporary SBAS outages during maintenance or faults.	Loss of LPV guidance [14].[1]
SouthPAN Outage	2023	Satellite hardware fault	Loss of hosted SBAS capability during pre-operational phase.	Temporary suspension of Open Services [15].

[1] In 2019, the FAA issued multiple WAAS service advisories and NOTAMs documenting temporary, localised loss of LPV guidance due to maintenance and system anomalies. These notices were operational in nature and are no longer publicly archived.

2.1.3 Electromagnetic Vulnerabilities

GNSS signals are transmitted from satellites that are 20,000 km away in Medium Earth Orbit (MEO). Their signals are incredibly weak by the time they reach the Earth and can be easily interfered with. One of the most pressing concerns is intentional radio frequency interference (RFI) of the EM spectrum. RF spectrum threats such as jamming, spoofing and meaconing (detailed below) represent a convergence of CEMA. Together these challenge the reliability and trustworthiness of PNT systems.

While these tactics are well-known in active conflict zones, jamming is also increasingly observed within grey-zone activities and even during peacetime operations. Having these disruptions bleed into peacetime represents a shift towards persistent and low-level interference that can disrupt civil, commercial and military users alike. Aviators and mariners have procedures to follow when GNSS becomes unavailable, and can in most cases navigate successfully using back up technologies to guide them through the area GNSS denial. However, in some cases, these occurrences lead to incidents and accidents. Selected high-profile examples of such incidents are summarised in Table 4.

Definitions

Jamming is the deliberate transmission of strong radio signals in the same frequency band used by GNSS. As GNSS signals are weak, a relatively low-power jammer can raise the noise floor enough to exceed their transmission amplitude. To the receiver, it appears as if the satellite signals have vanished, rendering it unable to acquire, track, or compute a position, velocity and time solution.

Spoofing goes further whereby actors transmit fake GNSS signals that deceive a receiver into computing a designed, incorrect time and/or location. Both are increasingly accessible to non-state actors due to the proliferation of low-cost equipment, where a simple simulator can cost a few hundred dollars on mainstream hobbyist websites. Daily incidents are recorded around the world, notably affecting aviation and maritime sectors.

Meaconing is the re-broadcasting of genuine GNSS signals, typically with slight delays or altered locations, to confuse or mislead receivers. Unlike spoofing, which generates false signals, meaconing uses real signals captured and re-emitted, making it harder to detect.

Table 4: Examples of high-profile GNSS jamming and spoofing incidents in chronological order.

Example	Location	Year	Description	Consequence
The Newark Jamming Event	Newark, USA	2012	Truck-mounted GPS jammer disrupted airport operations.	GBAS deployment delays; FCC enforcement action [16].
Stena Impero Spoofing Event	Strait of Hormuz, Iran	2019	AIS/GNSS spoofing misled navigation in Iranian waters.	Vessel and crew detained, maritime spoofing risk highlighted [17].
Denver Airport GNSS Disruption	Denver, USA	2022	Unintentional RF interference disrupted aircraft operations.	33-hour GNSS disruption near major airport [18].
Dallas Airport GNSS Disruption	Dallas, USA	2022	GNSS interference affected aircraft near Dallas airport.	24-hour disruption; source unidentified, intent unknown [18].
Sun Valley Approach Event	Idaho, USA	2023	GPS jamming caused aircraft deviation during approach.	Terrain-related risk; ATC intervention prevented accident [19].
Lyon Airport Jamming Event	Lyon, France	2023	Vehicle-based jammer disrupted airport operations.	Localised outages, jammer identified and fined [20].
AZAL Flight 8243 Shoot-down	Chechnya/ Kazakhstan	2024	GNSS jamming near Grozny during EW activity degraded navigation.	Aircraft shot down and crashed with 38 fatalities. Highlighted GNSS denial risks in conflict zones [21].
MSC Antonia Grounding Event	Red Sea, near Jeddah	2025	GPS spoofing caused vessel course deviation.	Port disruption, widespread regional spoofing impacts [22].

Several public reports have been published on the topic of GNSS jamming and spoofing, which may be used as a reference to the subject. These are summarised in Table 5 below.

Table 5: Public reports on GNSS jamming and spoofing.

Report Name	Organisation	Year	Notes
Sentinel Project – Report on GNSS Vulnerabilities.	Chronos Technology	2014	The report details a UK-wide trial of ground-based GNSS interference detection sensors, deployed to monitor jamming and spoofing across a range of real-world environments over a 12-month period [23].
Above us only stars "Exposing GPS spoofing in Russia and Syria".	C4ADS	2019	Investigation of deliberate GPS spoofing incidents primarily conducted by Russia, which affected commercial maritime and aviation traffic in the Black Sea, Crimea, and Syria [24].
GPS Spoofing Final Report.	OPSGROUP	2024	Report outlines the escalating threat of GPS spoofing in aviation, primarily related to conflict zones, noting a 500% increase in incidents, with approximately 1,500 flights affected daily by mid-2024 [25].
Report on GNSS Interference in the Baltic Sea.	GPS Patron, Gdynia Maritime University	2024	Six-month terrestrial monitoring study of GNSS jamming and spoofing in the Baltic Sea region affecting maritime operations [26].

2.2 Personnel Hazards

Personnel hazards may be the least recognised and acknowledged threat to PNT, but they can have major consequences for PNT resilience. These hazards can include both unintentional and malicious insider threats, as well as forms of foreign interference that exploit trusted personal or institutional relationships.

Insiders may include an organisation's employees, contractors, or third-party partners who have authorised access to critical systems and facilities [27]. This makes them uniquely positioned to exploit and/or expose vulnerabilities, whether intentionally or unintentionally, that are otherwise difficult for external actors to reach. Additionally malicious insiders could undertake espionage, sabotage, foreign interference and theft. These threats could manifest in PNT in a range of ways, including but not limited to the following:

- A malicious insider within a ground control centre could manipulate satellite control commands, interfere with time and orbit data uploads, or disrupt navigation messages.
- Insiders at telecommunications hubs or data centres responsible for GNSS augmentation services (such as SBAS or commercial correction networks) could deliberately tamper with signals, degrade service availability, manipulate timing references, or leak sensitive system data.
- Insiders may also act unintentionally, for example by mishandling sensitive cryptographic material, misconfiguring system software, or failing to follow established security protocols.

In some cases, incidents that may have originated from personnel hazards manifest instead as information or other hazard types once their effects materialise. In other more subtle instances, foreign interference can take the form of activities framed as civil assistance or PNT cooperation. Analogies in Table 6 illustrate how these indirect pathways can pose serious risks to Australia's PNT resilience.

Table 6: Examples of insider threats and foreign interference in space and energy sectors.

Example	Year	Sector	Description
NASA Johnson Space Center IT Damage	2017	Space - cyber	A former contractor retained remote access and damaged NASA IT systems after termination [28].
Power grid insider tampering	2016	Energy	Cases where compromised or misused operator credentials enabled unauthorised access to SCADA systems, disrupting grid operations [29].
BeiDou ground stations in Pacific island states	2022	Space / PNT infrastructure	Reports of BeiDou ground stations hosted at Chinese diplomatic sites in the Pacific, raising concerns over dual-use PNT infrastructure and foreign influence [30].

2.3 Supply Chain Hazards

Supply chain hazards are increasingly recognised as a risk to PNT resilience. Modern PNT systems depend on globally distributed supply chains spanning satellite manufacturing, ground infrastructure, user equipment, software, and cloud-based services. Disruptions or compromises at any point in this chain can propagate across multiple systems and sectors, undermining trust, availability, and integrity at scale. Unlike traditional RF interference, supply chain hazards are often hidden, difficult to detect, and embedded within trusted components and services. Each stage in the supply chain introduces potential vulnerabilities that can be exploited, for example:

- Hardware components could be tampered with before installation, introducing hidden functions or backdoors.
- Software libraries may be manipulated to insert malware or vulnerabilities.
- Dependence on single-source suppliers or foreign vendors for critical technologies also raises supply chain hazards.
- Supplying PNT-related goods and services to foreign companies with supply chains risks may also damage reputation or put an organisation at risk through secondary exposure to sanctions, export control breaches, contractual liability, or association with compromised or dual-use systems.
- Civil receivers are mass-produced often with limited security features, and may rely on third-party chipsets or firmware with opaque provenance. Compromised receivers could be susceptible to denial-of-service, false data injection, or data exfiltration.

As the examples in Table 7 illustrate, even an isolated satellite error can disrupt operations for civil aviation, maritime navigation, telecommunications, and other critical systems that rely heavily on uninterrupted PNT data. In some cases, failures have been short-lived and quickly corrected by system operators, while in others, the disruptions have persisted for hours or even days, affecting thousands of users worldwide.

Table 7: Examples of potential supply chain threats leading to GNSS outages and disruptions.

Event	Year	Type of event	Description	Consequence
GPS SVN-19 Clock Instability	1993	Satellite hardware fault	Early GPS Block IIA satellite with unstable onboard clock	Limited operational use, cautionary lessons for satellite clock design [31].
GPS Week Rollover Bug (1999)	1999	Legacy software design flaw	Receivers failed or output incorrect time due to 10-bit week counter rollover	Widespread legacy receiver issues [32].
GPS Week Rollover Bug (2019)	2019	Receiver software bug	Repeat of 1999 rollover affecting legacy receivers	Position and time faults in outdated devices [33].
NavIC Satellite Failures	2016-2025	Satellite and launch failures	Onboard clock and launch vehicle reliability issues	Reduced availability, fewer than 50% of satellites operational [34].

Supply chain impacts can become evident long after initial design, procurement, or deployment decisions are made. In the examples shown, vulnerabilities were embedded in hardware architectures or software assumptions that persisted across decades, only becoming visible when systems aged, scaled, or encountered boundary conditions. Such failures highlight the importance of lifecycle management, diversification, and continuous assurance across satellite, receiver, and software supply chains, particularly for PNT services that underpin safety-critical and nationally significant systems.

2.4 Physical Hazards

Physical hazards to GNSS encompass threats to satellites in orbit, the terrestrial infrastructure that controls and monitors them, and the user equipment that depends on GNSS services. These hazards may arise from unintentional accidents or deliberate hostile actions, and can result in immediate service disruption as well as longer-term degradation of PNT resilience.

Satellites are vulnerable to direct physical attack and unsafe proximity operations. Anti-satellite (ASAT) weapons tests conducted by China in 2007, India in 2019, and Russia in 2021 demonstrate the capability to physically destroy satellites, generating long-lived orbital debris fields and posing risks not only to the targeted systems, but to other space assets sharing similar orbital regimes. Beyond kinetic attacks, so-called co-orbital systems can manoeuvre in close proximity to GNSS satellites, raising concerns around hostile inspection, interference, or accidental collision, particularly in congested orbital environments. Table 8 provides illustrative examples of direct-ascent ASAT tests as a specific class of kinetic physical hazard, demonstrating how such actions can produce both immediate and long-term disruption to space-based PNT systems.

Table 8: Examples of direct-ascent ASAT tests as kinetic physical hazards to satellites.

Incident	Year	Category	Description
Chinese ASAT Test	2007	Space segment	China destroyed its Fengyun-1C weather satellite with a direct-ascent missile, creating over 3,000 trackable debris pieces highlighting the vulnerability of satellites in LEO/MEO [35].
Indian ASAT Test	2019	Space segment	India demonstrated a direct-ascent ASAT weapon, intercepting a satellite in LEO and raising concerns about debris and GNSS vulnerability [36].
Russian ASAT Test	2021	Space segment	Russia destroyed the Cosmos-1408 satellite, generating over 1,500 pieces of trackable debris [37].

ASAT incidents represent only one subset of physical threats in the space domain. Broader assessment of space threats, including co-orbital systems, rendezvous and proximity operations, and non-kinetic counter-space capabilities, is beyond the scope of this report. Comprehensive assessment of the full spectrum of space threats, including state and non-state counter-space capabilities has been done recently by the Center for Strategic and International Studies [38].

On the ground, GNSS control centres, uplink facilities, and monitoring stations represent critical nodes whose disruption can have system-wide effects. These facilities may be affected by deliberate actions such as sabotage, theft, or terrorist attack. Some Continuously Operating Reference Stations (CORS), timing facilities, and monitoring receivers, are often installed in exposed or remote locations, which can reduce the likelihood of overt physical attacks. However, their remoteness also means limited physical oversight, reduced monitoring, and delayed maintenance increasing the risk of covert interference, unauthorised modification, or undetected degradation. Physical damage to ground infrastructure can interrupt command and control functions, delay anomaly resolution, or prevent timely updates to navigation and timing data.

Physical hazards also extend to downstream user equipment. GNSS receivers embedded within critical infrastructure assets, such as ports, energy facilities, telecommunications sites, and transport systems, may be subject to vandalism, theft, or tampering, resulting in operational impacts.

Physical threats to GNSS span all segments of the system, from satellites in orbit to ground infrastructure and user equipment. The persistence of orbital debris, the concentration of critical ground facilities, and the widespread deployment of GNSS-dependent receivers mean that even isolated physical incidents can have cascading and long-lasting impacts on PNT services and the sectors that depend upon them.

2.5 Natural Hazards

GNSS signals are vulnerable to a range of natural phenomena that can degrade performance or cause service outages. These hazards are predominantly driven by space weather and atmospheric dynamics that are outside human control.

Solar flares, coronal mass ejections, and geomagnetic disturbances can alter ionospheric conditions. This can increase signal delay, scintillation, and orbital drag, and thereby degrading GNSS performance. During severe geomagnetic storms, these effects can intensify, leading to substantial positioning errors, degraded timing reliability, or even temporary loss of signal lock, as illustrated by historical events as shown in Table 9.

Table 9: Examples of natural threats to PNT.

Incident	Year	Category	Description
Halloween solar storms	Oct-Nov 2003	Solar storms / space weather	Severe ionospheric disturbance led to WAAS precision-approach unavailability for parts of North America during peaks of the storms [39].
St. Patrick's Day geomagnetic storm	Mar 2015	Geomagnetic storm	Documented GNSS degradation, large ionospheric disturbances and positioning accuracy impacts [40].
Geomagnetic storm (high latitudes)	Sep 2017	Polar ionospheric scintillation	Strong scintillation and loss-of-lock events observed. Demonstrated vulnerability of GNSS in disturbed polar ionosphere [41].
G5 geomagnetic storms	May 2024	Severe geomagnetic storm	NOAA reported the strongest storm in decades. WAAS LPV coverage dropped to zero on 11 May. Widespread user reports of degraded GPS accuracy [42].

Ionospheric scintillation refers to rapid fluctuations in electron density that cause GNSS signals to fade, distort, or fluctuate in phase and amplitude. While low-level scintillation is a persistent feature of the equatorial and high-latitude ionosphere, its severity, spatial extent, and temporal persistence can increase significantly during geomagnetic storms, transforming a background environmental condition into an operational hazard for PNT systems.

In equatorial and low-latitude regions, severe space-weather events can trigger the formation of large-scale plasma density irregularities commonly referred to as *equatorial plasma bubbles*. These structures arise from post-sunset ionospheric instabilities and can grow rapidly, extending over hundreds of kilometres in longitude and altitude. Recent observations show that during intense geomagnetic storms, plasma bubbles can become unusually deep, widespread, and long-lived, in some cases persisting into daytime hours when GNSS services are typically most reliable [43].

Such storm-enhanced plasma bubbles produce strong amplitude and phase scintillation, leading to frequent GNSS loss-of-lock events, degraded positioning accuracy, and unreliable timing outputs. This has direct implications for the availability and continuity of augmentation services such as Australia and New Zealand's SBAS (SouthPAN), particularly for Safety-of-Life (SoL) aviation operations in northern Australia. SouthPAN services can be affected for locations under the equatorial ionisation anomaly, as their exposure to these effects increases [44].

Figure 1 below shows the map of SouthPAN coverage of Australia and New Zealand. The areas shown in green indicate regions covered for SoL aviation procedures, while areas in blue in northern Australia are not covered for SoL services due to proximity to the equator and elevated ionospheric activity.

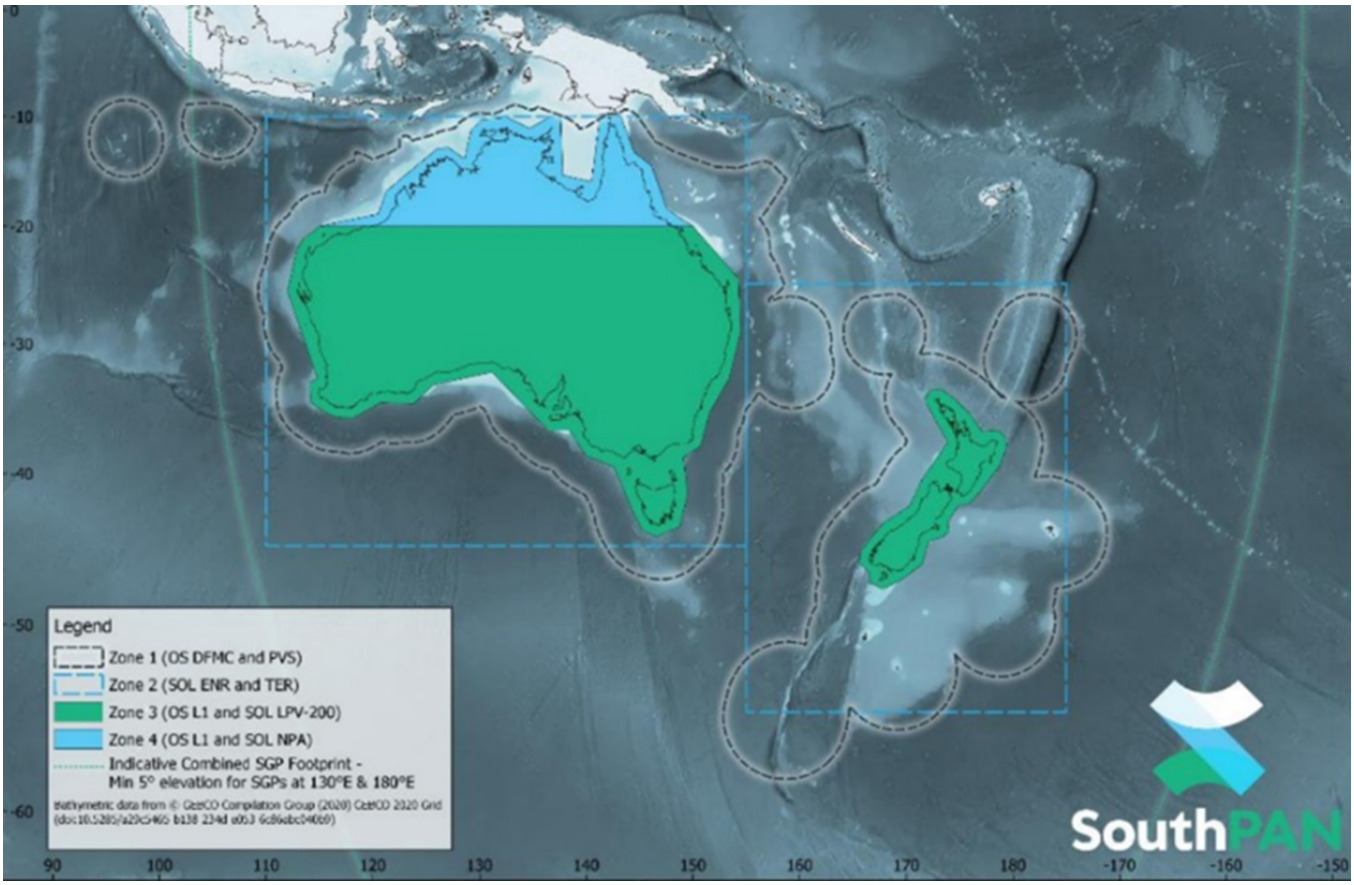

Figure 1: Map of SouthPAN coverage (Source: Geoscience Australia).

2.6 Chapter Summary

Threats to PNT services can arise from a wide range of sources, including deliberate interference, system and supply chain failures, personnel hazards, physical attacks, and natural phenomena. Although these threats may differ in origin and intent, they often and similarly result in adverse impacts to PNT information and PNT systems operations.

This in turn results in degraded accuracy, loss of service availability, and reduced trust in PNT-dependent systems across defence and critical infrastructure sectors. Australia's lack of a national PNT framework further makes it difficult to assign ownership of threat response and mitigation. Chapter 3 follows by examining how PNT threats may arise and evolve across frameworks familiar to both Defence and civil government.

3 PNT THREATS ACROSS THE COMPETITION SPECTRUM

This chapter examines how PNT-related hazards evolve across the cooperation-competition-conflict spectrum. Some PNT disruptions occur as isolated technical events, while others might interact or be leveraged for asymmetric gain. This section examines how hazard classes might interact and accumulate, to provide Defence, Home Affairs, and other critical national stakeholders with a view to understand how PNT threats could eventuate within Australia's strategic environment.

3.1 Cooperation-Competition-Conflict Spectrum

Australian government agencies may approach PNT threats with differing perspectives. The Australian Defence Force (ADF) focuses on assured PNT for mission operations and assurance, while the Department of Home Affairs (DHA) views PNT from the perspective of impacts to critical infrastructure, essential services, and broader national security. In recognising that many PNT threats are non-discriminatory and can affect both civil and military sectors concurrently, aligning these perspectives would help develop an integrated civil-military response to these threats.

PNT threats can occur in peacetime, in war, and in the grey zone between them. They can occur during routine activity, or emerge during periods of geopolitical tension or deliberate interference. This section applies the hazards-based approach (described in Chapter 2) to the cooperation-competition-conflict spectrum (referred collectively as the competition spectrum), a framework used in defence planning, to provide a combined civil-military perspective on how PNT threats manifest across strategic conditions. This approach is intended to help Defence prioritise investment and program planning based on PNT threat consequences and operational risk, while supporting alignment with broader government responsibilities for national resilience.

While the peace-war distinction is well established within the ADF doctrine, in practice, Defence must contend with activities that do not sit neatly within this framework. In the current strategic landscape, many threats to Defence and to Australia occur in the space between cooperation and conflict, commonly described as the competition phase and often referred to as the grey zone [45, 46]. This framing is particularly relevant to PNT, where many disruption or interference events occur outside of active conflict and align with grey-zone behaviours. While the competition spectrum is primarily a military concept, interpreting PNT within this framework is relevant not only to Defence, but also to Home Affairs, and other national security stakeholders.

Definitions (adapted from [45]):

Cooperation: Creation of power and influence without damaging or violent interactions. Positive engagement for mutual benefit.

Competition: Rivalry between actors seeking to outperform other competitors. Contest is the constant condition.

Conflict: A temporal condition of competition characterised by war.

3.2 PNT Threat Matrix

Table 10 presents a threat matrix that maps representative PNT hazard vectors across the cooperation-competition-conflict spectrum. The mapping illustrates how similar underlying hazards can manifest as benign, ambiguous, or hostile forms depending on context and intent. This provides a structured basis for understanding how PNT-related activities and disruptions evolve across phases of competition.

Table 10: Examples of PNT activities, disruptions, and threats across the competition spectrum.

Hazard / spectrum	Cooperation	Competition	Conflict
Cyber, EM, Information	• Identification of SouthPAN data integrity issues through testing and validation • White-hat testing and simulation of timing-dependent SCADA systems	• GNSS jamming in the South China Sea affecting ports, maritime operations, aviation • Low-visibility cyber intrusions across PNT space, ground, and user segments	• Deliberate GNSS spoofing and interference by state actors • Coordinated cyber-EM attacks on PNT systems during active conflict
Personnel	• Temporary GNSS outage caused by authorised ground segment maintenance • Routine use of navigation systems by personnel, including access to sensitive locations	• Exploitation of legitimate personnel access for dual-use or covert PNT-related activities • Insider use of authorised access to collect information on PNT systems	• Insider sabotage or interference at GNSS ground or control facilities • Deliberate disruption of PNT services by compromised personnel to gain operational advantage
Supply chain	• Mergers, acquisitions, and ownership changes involving PNT suppliers and manufacturers • Commercial sourcing decisions that introduce hidden dependencies or single points of failure	• Introduction of compromised or degraded components into PNT equipment supply chains • Coercive leverage over suppliers through economic pressure, regulation, or market access	• Denial of access to critical PNT components, spares, or software updates • Deliberate disruption of PNT supply chains to degrade or disable operational capability
Physical	• Physical security assessments and risk management of PNT infrastructure and assets • Routine inspection, surveying, and access for maintenance or safety assurance	• *Accidental* damage to PNT-related infrastructure, such as subsea cables relaying timing data • ASAT tests and in-orbit rendezvous operations in proximity to GNSS satellites	• Deliberate physical destruction of GNSS ground network due to hostilities • Missile strikes on energy infrastructure causing flow-on impacts to network operations
Natural	• Unpredictable space weather or natural disaster events causing temporary degradation of PNT services • Persistent environmental conditions (e.g., ionospheric phenomena) affecting PNT performance	• Exploitation of natural hazard events to mask or amplify PNT interference or intrusion • Strategic provision of PNT assistance during crises to create dependence or influence	• Natural hazards compounding or amplifying the impacts of PNT disruption during conflict • Reduced resilience and recovery of PNT services in contested environments

Some entries in the cooperation column are routine activities rather than threats in themselves, for example business mergers and acquisitions. However, they represent the types of interactions or dependencies that create vulnerabilities if conditions evolve towards competition or conflict, such as the withholding PNT component supplies for advantage or disadvantage. Market and technology drivers may also include factors like widespread use of AI. Whilst generative AI can be employed for PNT situational awareness (discussed in Section 5.6), it can also be deployed to create, evolve, or accelerate other threats to PNT in contested environments.

Other examples reflect how the same hazard vector can interact and accumulate across the spectrum, such as illustrated broadly in Figure 2. For example, natural hazards such as space weather can affect PNT services in all phases of the spectrum regardless of intent. However, space weather effects can be amplified during the competition and conflict phases, and provide the opportunity for malicious effects to layer and accumulate. The threat matrix therefore describes how each hazard type may manifest in practice across different strategic conditions, rather than implying that all activities are threats, or that each example is equivalent in severity.

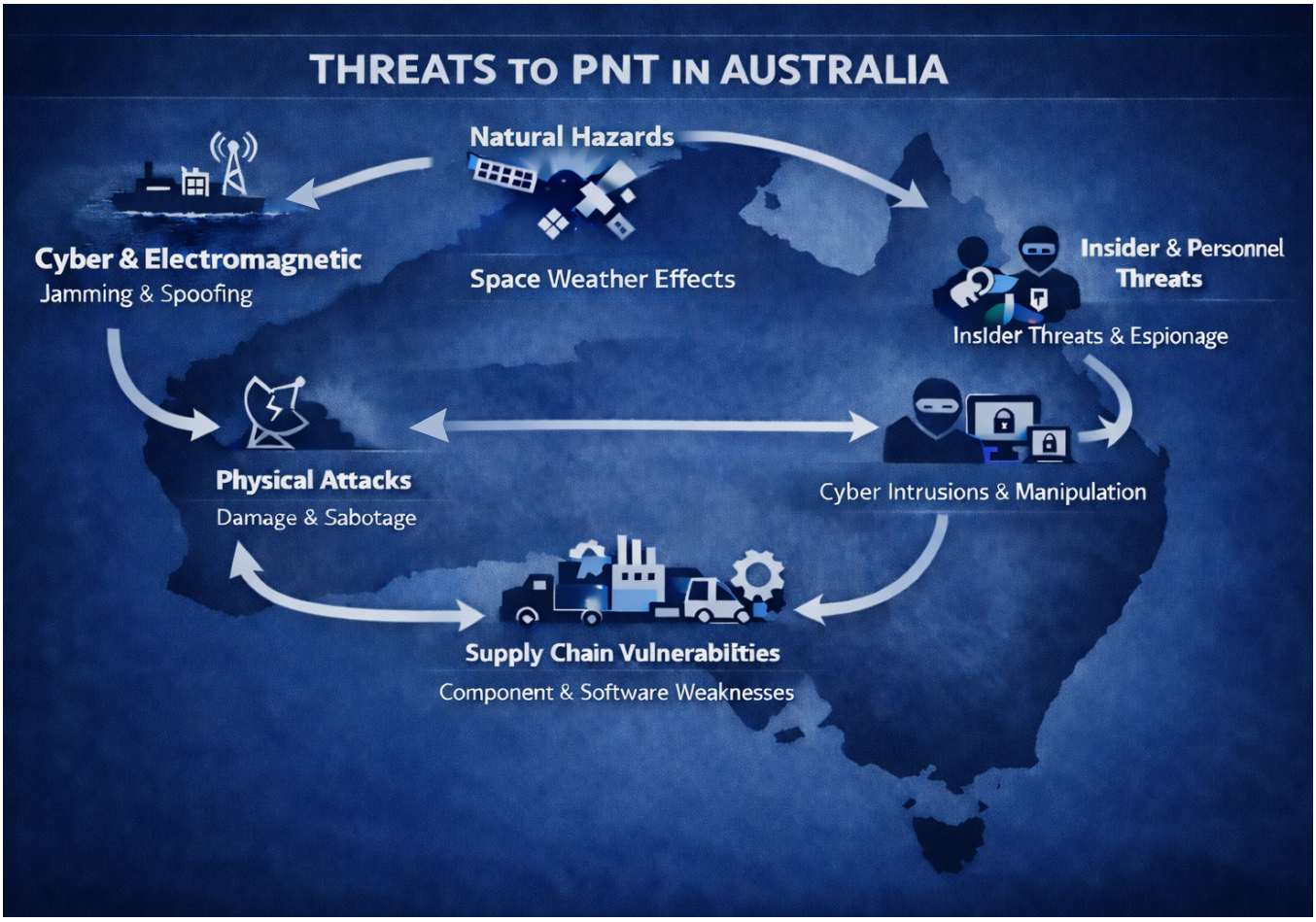

Figure 2: PNT-specific threats across hazard domains impacting Australia. Note: elements of this image were AI-generated.

What is important to note is that PNT-related hazards do not always appear discretely within individual phases of competition. As illustrated in Figure 3, PNT activities and threats present in the cooperation phase can also occur in competition, and those in competition can continue in conflict. Rather than replacing one another, threats can accumulate across the spectrum, with changes in intent, visibility and consequence.

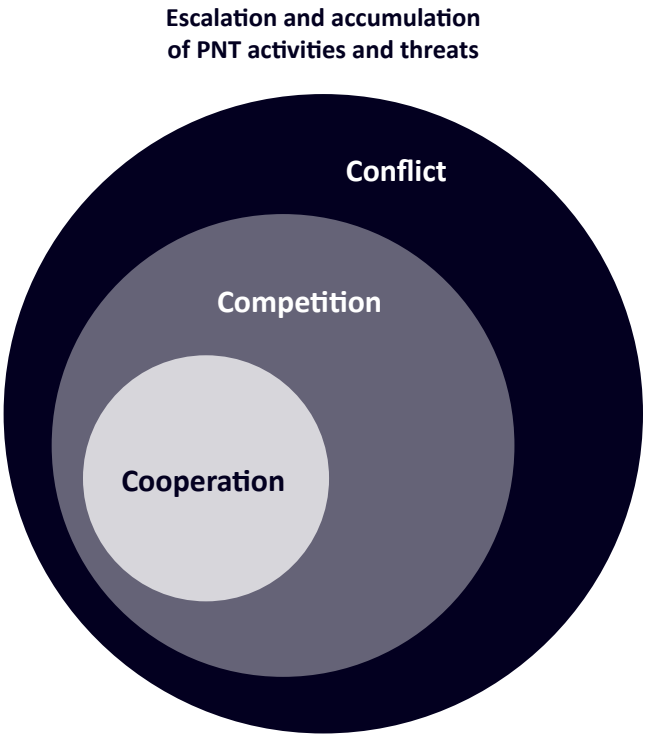

Figure 3: PNT threats in the cooperation phase can also manifest in competition, and those in the competition can continue or intensify in conflict.

In reality, different aspects of Australia's national system may occupy different positions along the competition spectrum simultaneously. For example:

- Defence domains can be in competition while civilian sectors remain in cooperation.
- Different critical infrastructure sectors may experience different pressures for PNT resilience.
- Natural hazards do not align with geopolitical phases.
- Adversaries may exploit sectors, industries, or individual organisations with less resilience.

The diagram therefore reinforces the global PNT community's call for national and government institutions to treat PNT resilience as a continuous requirement spanning peacetime operations, grey-zone competition, and conflict.

3.3 PNT Threat Consequence

While the threat matrix provides a view of how hazards emerge, evolve, or accumulate, it does not in itself indicate which disruptions are most consequential in terms of operational impact, national security, and public safety. Similar hazard vectors can produce different outcomes depending on scale, duration, affected sectors, and the ability of institutions to respond. It is therefore necessary to consider the consequence of PNT threats and how they translate into impacts for Defence, critical infrastructure, and the Australian public.

The analysis that follows deliberately focuses on consequence rather than full risk quantification. While risk is commonly understood as a function of threat, vulnerability, and consequence [47], consequence provides a useful first-order lens for comparing the potential severity and breadth of effects across different hazard classes. This highlights where PNT disruptions would have the greatest significance, without duplicating detailed scenario-based or vulnerability-driven risk analysis.

3.3.1 Analysis Methodology

A customised framework was developed by FrontierSI to categorise the consequence of PNT threats against a set of critical factors. FrontierSI adapted and customised an approach by Paladin to categorise the threat consequence across several critical factors [48]. This method allows for a more structured analysis of the impact of each threat or activity, and closely follows that presented in FrontierSI 2024 report *Assessing PNT Disruptions and Their Impacts on Defence* [3].

FrontierSI developed tailored guidance to support consistent assignment of a Consequence rating for each critical factor. Each threat / activity was rated across critical factors with a corresponding score (1-5), then a non-weighted average applied to attain an overall Consequence score. These critical factors reflect impacts to Defence, critical infrastructure, and public safety.

Critical factors

Critical infrastructure:

- Does the event disrupt national coordination or governance?
- Does it stop of severely degrade enterprise operations?
- Are impacts localised or systemic?

Defence situational awareness

- How many Defence domains lose C5ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance) capability?
- Is situational awareness degraded or lost entirely?
- Are decision timelines or operational tempo constrained?

Public perception and safety

- Is there loss of life?
- Is civil unrest likely?
- Is public confidence in institutions affected?

Table 11 below defines the consequence scale used in this assessment, where qualitative impacts across Defence situational awareness, critical infrastructure, and public perception and safety are described.

Table 11: Consequence scale used for scoring.

Consequence (Score)	Defence situational awareness	Critical infrastructure	Public perception and safety
Severe (5)	C5ISR disabled across all Defence domains. No situational awareness. Mission execution impossible. Likelihood of multiple concurrent threats.	National coordination and communication disabled. Enterprise and social systems not functioning. National governance mechanisms fail. National security compromised.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised. Significant structural adjustment required.	National coordination degraded. Enterprise and social systems overwhelmed. National governance mechanisms degraded.	High public fear and insecurity. Loss of confidence in government. Serious casualties and fatalities. Defence required to manage unrest.
Moderate (3)	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Business-as-usual coordination not possible. Noticeable degradation of enterprise and social systems. National governance partially impaired.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Minor impact on 1-2 domains. C5ISR degraded, but functional via alternatives. Minor mission impacts.	Coordination hindered but workarounds available. Minor degradation to enterprise and social systems. Localised governance and decision-making impacted.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Negligible impact. Systems cope without major change. Decisions escalated through normal governance.	Public concern is minimal. Only minor injuries. No long term effects.

3.3.2 Consequence Assessment Results

Each threat example from the PNT threat matrix (Table 10) was assessed against the critical factors, and assigned a consequence score between 1 and 5 for each dimension. A non-weighted average was then applied to derive an overall Consequence score (Table 12). The mean Consequence score applies to each activity or threat cell, and does not represent compounded effects across multiple cells or hazards. Raw results of the scoring are presented in Appendix A.

This method provides a consistent basis for comparing the consequences of the PNT threats across the competition spectrum. Note, this exercise intentionally focuses on consequence and does not assign PNT threat likelihood values, which would vary across adversaries, scenarios and operational contexts.

The mean consequence scores are also presented as line plots (Figure 4), which illustrates how the consequences associated with each hazard type could escalate from cooperation to competition to conflict. While the scores have been derived from specific examples and are subjective, they enable a useful high-order interpretation of how PNT threats may evolve as strategic environments change.

Table 12: Mean consequence scores for PNT hazard types across the cooperation-competition-conflict spectrum.

PNT hazard types / conflict spectrum	Cooperation	Competition	Conflict
Cyber, EM, information	2.0	2.0	3.7
Personnel	2.3	2.3	3.7
Supply chain	1.0	3.3	4.0
Physical	1.0	2.3	5.0
Natural	3.0	4.0	5.0

Consequence escalation across the competition spectrum

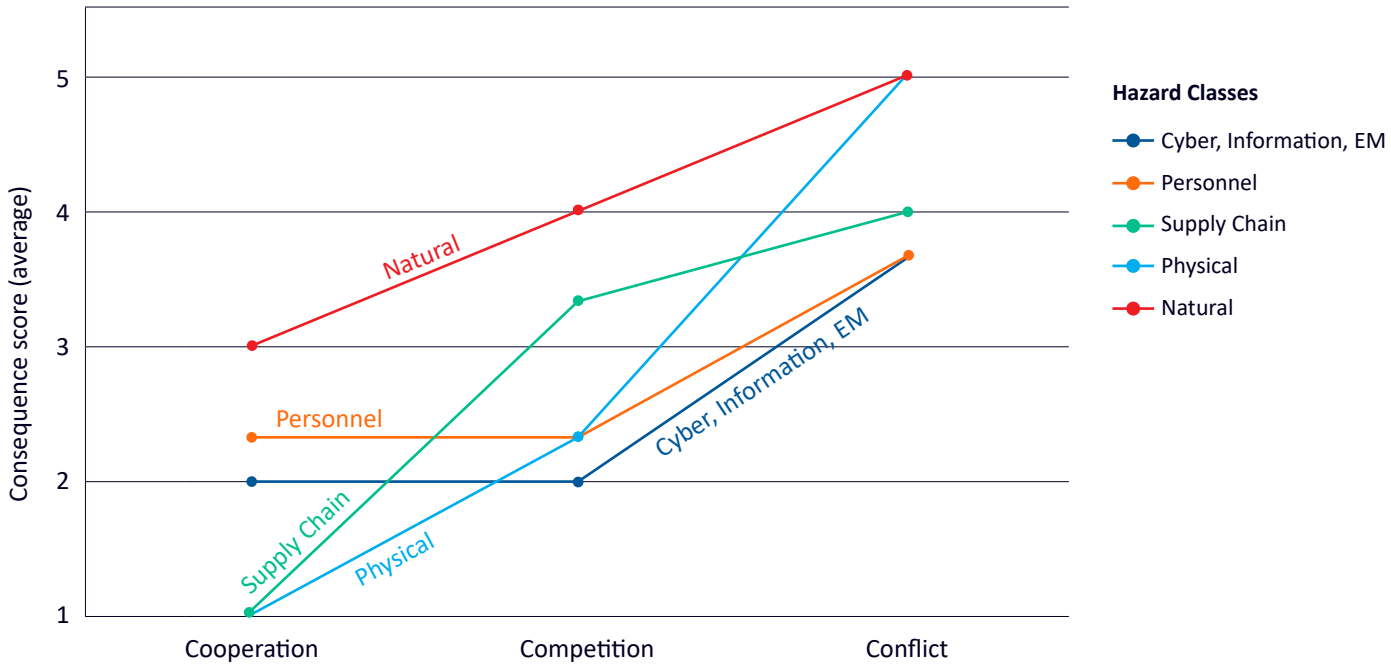

Figure 4: Line plot illustrating escalation of PNT threat consequence across the cooperation-competition-conflict spectrum.

The following observations and interpretations are made regarding the consequence scores and escalation trends:

- Natural hazards demonstrate a high baseline consequence even in cooperation. The impacts of space weather are broad and not targeted at any specific group or asset, and can result in higher inherent disruption.
- Physical hazards may quickly escalate during competition and conflict, where kinetic means are employed to degrade infrastructure assets and hence the availability and integrity of PNT information.
- Supply chain hazards may escalate rapidly during competition and conflict. They are attractive vulnerabilities for adversaries seeking advantage in the grey zone, or aiming to degrade Australia's national capability during conflict.
- Cyber, information, and EM hazards are persistent across all phases. Based on current cyber and EM incidents and attacks, it can be inferred that state and non-state actors attempt to keep activities under the attribution threshold. It can be assumed that effects of such attacks may be compounded during competition and conflict, creating sustained disruption to critical infrastructure and causing social disruption. During conflict, cyber effects by themselves may not cause severe consequences, but can act as a force multiplier such as for kinetic operations (i.e. physical hazards) or supply chain disruptions.
- Personnel hazards are also persistent across all phases. Insider access, human error, or coercion can be exploited without escalating to conflict, though may produce limited severe consequences on their own. During cooperation and competition, these are among the more consequential hazards due to their potential to facilitate unauthorised system access or exploitation. Their impacts could be more pronounced in conflict, creating opportunities to layer on or compound other threat types.

3.4 Implications for Defence and Home Affairs

Implications of the consequence assessment are synthesised for Defence representing the military authority on PNT, and Home Affairs representing the broader civil government on critical infrastructure risk management, including PNT. The following tables (13-17) aim to provide a view of how each hazard type could be deterred, institutional impacts, and high-level mitigation priorities from governance, operational, industrial and/or technical perspectives.

Table 13: Institutional implications of natural PNT hazards for Defence and Home Affairs.

Natural Hazards		
	Defence	**Home Affairs**
Consequence	Natural hazards present the highest baseline consequence for PNT due to their broad, non-discriminatory impacts across both Defence and civilian systems, with potential to simultaneously degrade military C5ISR and civilian critical infrastructure at national scale.	
Deterrence	Space weather and other natural hazards cannot be deterred through adversary-facing measures and must be treated as an unavoidable operational condition.	
Implications	Defence should assume that space-based PNT degradation or denial will occur and loss of PNT information should be treated as a baseline planning factor.	Impacts can extend across multiple critical infrastructure sectors simultaneously, creating coordination and prioritisation challenges.
Mitigation	Defence should provide proportionate focus on assured PNT for the warfighter, as well as resilient PNT for the non-warfighting systems it depends on. Mission operations and assurance depend on the ability to rapidly transition to alternative capabilities, supported by multi-layered PNT.	National-level PNT situational awareness is required, including timely information sharing across jurisdictions and sectors. Critical infrastructure entities should ensure redundancy and diversity in PNT sources. Establishing national PNT infrastructure as a public good, that can be accessed by multiple sectors and user types, could contribute to mitigation. Investment in preparedness, redundancy, and transparent response frameworks can reduce vulnerability and public impact.

Table 14: Institutional implications of physical PNT hazards for Defence and Home Affairs.

Physical Hazards		
	Defence	**Home Affairs**
Consequence	During competition and conflict, physical hazards represent the highest operational consequence for Defence as they can rapidly and deliberately degrade PNT infrastructure and systems, leading to acute loss of C5ISR. Unlike natural hazards, physical attacks are targeted and adversary-driven, with impacts that may be localised initially, but escalate quickly through dependency chains.	
Deterrence	Physical attacks on PNT systems can be partially deterred through resilience and denial measures, including redundancy, hardening, and multi-layered PNT architectures that reduce the effectiveness of kinetic or destructive actions.	
Implications	Physical hazards pose the highest operational risk due to their potential to rapidly degrade PNT-dependent C5ISR during competition and conflict.	Physical hazards to PNT-enabled infrastructure can have cascading impacts across multiple critical infrastructure sectors, even when initial damage is geographically limited.
Mitigation	Mission operations and assurance depends on the ability to operate in contested and degraded PNT environments, and the use of multi-layered PNT solutions to quickly reconstitute degraded capabilities.	Strengthening the resilience of PNT-related infrastructure and ensuring redundancy and diversity in PNT sources is critical for reducing national-level impacts.

Table 15: Institutional implications of cyber, information and EM hazards PNT hazards for Defence and Home Affairs.

Cyber, Information and EM Hazards		
	Defence	**Home Affairs**
Consequence	Cyber, information, and EM hazards can occur across all phases of the competition spectrum, often persistently below the threshold of conflict.	
Deterrence	Some cyber and EM activities could be deterred through hardening of enabling PNT systems, although complete deterrence could be unlikely due to low barriers to entry by adversaries.	
Implications	The significance of these hazards lies in their potential to act as force multipliers, compounding other PNT threats or creating conditions for follow-on cyber or physical attacks.	These hazard types can generate widespread social and economic impacts without crossing the threshold of conflict. Their ambiguous and often unattributable nature complicates national response coordination and public communication.
Mitigation	Requires continuous PNT monitoring, anomaly detection, and cyber and EM hardening. Where appropriate, Defence should integrate complementary and alternative PNT technologies to sustain operational effectiveness in contested environments.	Requires enhanced national PNT situational awareness, including visibility of how cyber and EM disruptions affect PNT-dependent services across sectors. Civil operators would benefit significantly from access to PNT alternatives that are scalable, affordable, and not require complex retrofitting of systems.

Table 16: Institutional implications of supply chain hazards for Defence and Home Affairs.

Supply Chain Hazards		
	Defence	**Home Affairs**
Consequence	Supply chain hazards represent a hidden and compounding risk to PNT, driven by structural dependencies on upstream manufacturing, software, logistics, and specialist components. Exposure is shared across Defence and civilian sectors, but consequences are anticipated to increase as competition increases.	
Deterrence	Supply chain exploitation can be partially deterred by reducing adversary leverage through trusted partnerships, interoperability, diversification of suppliers, and assured access to critical PNT components.	
Implications	Mission and platform sustainment risks. Exploitation by adversaries of upstream dependencies in shipping, software, manufacturing, and logistics.	Amplified economic and societal impacts due to widespread civilian reliance on PNT-enabled services.
Mitigation	Strategic partnerships, interoperability, diversification, and assured access to critical PNT components.	Policy-led supply chain assurance, cross-government visibility, sovereign capability assessment, and support for domestic manufacturing where critical.

Table 17: Institutional implications of personnel hazards for Defence and Home Affairs.

Personnel Hazards		
	Defence	**Home Affairs**
Consequence	Personnel hazards constitute a continuous, low-visibility risk across all phases of the competition spectrum, arising from human access to PNT systems, data, and decision-making processes. Exposure is broadly shared across Defence, industry, and civilian critical infrastructure operators.	
Deterrence	Deterrence is less so through employing any specific PNT technology means, but depends primarily on good governance such as personnel vetting, counter-intelligence, and access controls.	
Implications	Insider risks in both design, capability acquisition and sustainment and Defence industry leading to espionage and foreign interference. Heightened during periods of geopolitical tension.	Insider risks within critical infrastructure operators leading to foreign interference. Heightened during periods of geopolitical tension.
Mitigation	Requires strong personnel security frameworks, continuous monitoring, security-by-design in PNT-enabled systems, and close engagement with Defence industry partners.	Requires cross-sector governance mechanisms, insider-threat awareness programs, information sharing, and regulatory enforcement across critical infrastructure operators.

Both civil and Defence aspects in Australia face overlapping threats to PNT and consequences that cannot be managed in isolation. While the form and visibility of disruption may vary between natural, physical, cyber, supply chain, and personnel hazards, their effects frequently converge on common outcomes. These include impacts on the integrity and availability of PNT signals, degraded situational awareness, impacts to mission operations, coordination of response efforts, and public safety and wellbeing. Accumulation and layering of high-consequence hazards creates a requirement for a national PNT response to disruptions, and alignment of investments across agencies.

3.5 Chapter Summary

PNT threats can evolve and accumulate across the competition spectrum. Natural hazards establish a persistent, non-discriminatory baseline risk that cannot be deterred and must be managed through preparedness and response. Physical hazards represent the most acute escalation of consequence during conflict, with the potential for rapid and severe degradation of C5ISR and critical infrastructure. Cyber, information, and EM hazards are characterised by persistence and adaptability, acting as force multipliers that erode trust and situational awareness over time. Supply chain hazards exploit both system interdependencies and economic leverage, while personnel hazards introduce continuous, low-visibility risks rooted in human access and governance. High-level hazard- or threat-driven recommendations are developed to identify a mix of governance, industrial policy setting, system hardening, and technological diversity. These are not exhaustive but are intended to illustrate the different levers that can contribute to Australian PNT resilience.

Part II of the ANCHOR report deep dives into situational awareness of PNT threats with a focus on RF interference, which can is still the most observable and obvious threat to PNT availability and integrity. It follows by presenting a comprehensive range of existing and emerging PNT technologies, before synthesising relevant architectures for Australia.

PART II: STRENGTHENING AUSTRALIA'S PNT RESILIENCE

4 PNT THREAT DETECTION AND RESPONSE

This chapter addresses PNT threat detection and response as an operational and decision-support capability, rather than a purely technical monitoring function. For Defence and other operators of critical infrastructures, the ability to detect, interpret, and respond to threats affecting PNT is fundamental to maintaining freedom of action, mission assurance, and safe operation in contested, degraded, and ambiguous environments. In practice, PNT disruptions are rarely binary. Instead, they are often partial, localised, intermittent, or deliberately deceptive, creating conditions in which systems continue to produce outputs that appear valid, but are increasingly untrustworthy. Without an explicit threat detection and response capability, such degradation may go unnoticed until it manifests as operational failure. For Defence, PNT threat detection and response is not simply a monitoring function, but a prerequisite for mission assurance, force protection, and freedom to manoeuvre in environments where GNSS disruption may be deliberate, localised, intermittent, or deniable.

This chapter focuses on threats to PNT that manifest within the RF domain, as these represent the most immediately observable, measurable, and operationally disruptive class of PNT hazards in contemporary operating environments. It concentrates on both intentional and unintentional RF interference affecting GNSS and related PNT signals, including jamming, spoofing, meaconing, and other forms of signal disruption. RF-based threats are prioritised because they are widely employed in grey-zone and hybrid activities, can affect large geographic areas simultaneously, and frequently impact both civil and military users without clear attribution or warning.

While the scope of this chapter is deliberately limited to RF-based PNT threats and their detection and response mechanisms, this reflects a conscious analytical and practical scoping decision rather than a judgement on the relative importance of other hazard classes. RF-mediated threats represent the common hazards affecting PNT today, with mature sensing, localisation, and response techniques available to support situational awareness and decision-making. In contrast, other PNT risk categories, such as cyber compromise of downstream systems, personnel and insider threats, supply-chain vulnerabilities, satellite or ground-segment failures, and natural hazards including space weather, require fundamentally different detection, attribution, and governance approaches. Addressing these coherently would necessitate distinct analytical frameworks beyond the scope of this report.

While many PNT situational awareness concepts have been developed in European and UK contexts, their relevance extends strongly to the Asia-Pacific region. Australia's geographic scale, reliance on satellite-based PNT across remote and maritime domains, proximity to equatorial ionospheric disturbances, and increasing exposure to GNSS interference in congested RF environments create a compelling operational case for enhanced PNT situational awareness.

The approaches discussed in this chapter provide a foundation for monitoring, understanding, and responding to PNT disruptions across civil, commercial, and national security applications in Australia and the broader APAC region. The region encompasses vast maritime approaches, dense shipping lanes, contested and congested RF environments. It is also characterised by a growing reliance on satellite-based PNT for navigation, surveillance, logistics, and humanitarian assistance and disaster response across the Pacific. Australia also plays a central role in supporting PNT-dependent services and infrastructure for neighbouring Pacific Island states, many of which have limited local redundancy or monitoring capability. In this context, situational awareness of PNT performance and disruption is not only a domestic resilience concern, but a regional enabler for coordination, assurance, and trust in shared PNT-dependent services.

PNT threat detection and response is framed in this chapter through the lens of situational awareness in dynamic systems, encompassing the ability to detect anomalous conditions, comprehend their operational significance, and anticipate their likely evolution in time and space. Building on established frameworks for PNT situational awareness (PNT-SA), this chapter adopts an SA-based construct for framing PNT threat detection and response [49]. This framework synthesised operational experience, resilience engineering principles, and established human-factors models of situational awareness to propose a structured approach comprising three interrelated levels, namely Perception, Comprehension, and Projection. These concepts are described below, noting that Comprehension is further divided into two parts - Substantial Threat Localisation and Characterisation, and Spectrum Policing and Interdiction:

2. **Perception –** spectrum situational awareness, involving the detection of RF anomalies over wide areas through continuous monitoring of the electromagnetic environment.
3. **Comprehension –** interpretation and understanding of the meaning of observed anomalies in context, including:
    a. Substantial Threat Localisation and Characterisation, which focuses on identifying and describing the source, nature, and extent of radio-frequency interference; and
    b. Spectrum Policing and Interdiction, which enables active enforcement, mitigation, and coordinated response where appropriate authorities and mechanisms exist.
4. **Projection –** anticipating future states and outcomes based on current understanding, transforming detection from passive monitoring into actionable foresight. Projection supports forecasting how interference may persist, intensify, or propagate across regions, and informs timely decisions on mitigation, operational adaptation, or escalation.

Together, these elements position PNT threat detection and response as a situational awareness-driven function that bridges technical sensing with operational decision-making. Rather than treating interference events as isolated technical anomalies, this approach enables Defence and other stakeholders to assess trust in PNT outputs, understand second-order impacts, and respond proportionately to evolving threats across tactical, operational, and strategic timescales.

4.1 Perception – PNT Situational Awareness

At the perception level, PNT-SA is defined as the ability to detect anomalous conditions in the RF environment that may indicate degradation, disruption, or manipulation of PNT services. For Defence and other operators of mission-critical systems, this capability provides the earliest indication that PNT conditions are contested or degrading, underpinning trust in navigation, timing, and synchronisation data before impacts propagate into operational failure or unsafe conditions. Perception therefore represents the foundational layer of PNT situational awareness, enabling timely recognition that something is wrong, even where the nature or source of the threat is not yet understood. Increasingly, this perception layer is supported not only by specialised PNT-SA systems, but also by relatively low-cost tools that enable users, operators, and local authorities to detect anomalous RF conditions indicative of PNT disruption.

In the context of GNSS and related PNT services, perception-level situational awareness (i.e., the initial detection of anomalous conditions in the RF environment) is particularly challenging due to the inherently weak nature of satellite signals, which are typically received well below the ambient noise floor. Detecting interference therefore requires the ability to sense both nominal GNSS signals and anomalous emissions across the same frequency bands, often in the presence of complex propagation effects, multipath, and legitimate high-power transmissions. Modern PNT-SA systems draw on advanced RF sensing techniques adapted from radar, electronic warfare, and radio astronomy to continuously monitor wide swathes of spectrum and identify deviations from expected signal behaviour.

Importantly, perception-level situational awareness is not concerned with attribution or intent, nor with precise localisation of interference sources. Its primary function is to detect the presence of anomalous RF activity and to provide sufficient confidence that PNT conditions may no longer be reliable. Determining what the interference is, where it originates, and how it should be addressed are functions of higher-level comprehension and response processes discussed in subsequent sections. Maintaining this distinction is critical to avoid conflating early detection with threat characterisation or enforcement.

Perception relies on a range of complementary measurement approaches that enable anomalous emissions to be detected and broadly characterised in terms of direction, timing, frequency behaviour, relative power, and inferred impact. These approaches include angular, temporal, frequency-based, and power-based techniques that exploit spatially distributed RF sensors and, in some cases, moving observation platforms. The underlying principles of these techniques, such as Angle of Arrival (AOA), Time Difference of Arrival (TDOA), Frequency Difference of Arrival (FDOA), and Power Difference of Arrival (PDOA), are introduced here at a high level and are described in more detail in Section 4.2, where their role in threat localisation and characterisation is examined.

In addition, perception-level awareness may be augmented through the indirect use of non-PNT data sources, such as Automatic Dependent Surveillance-Broadcast (ADS-B) and Automatic Identification System (AIS), where anomalies in aircraft and ship navigation behaviour provide indicators of GNSS interference affecting airspace users.

Effective PNT-SA can be achieved from multiple vantage points. Ground-based sensor networks provide persistent, high-sensitivity monitoring of the RF environment, particularly for low-power, localised interference sources that operate close to the horizontal plane. These systems are well suited to detecting subtle degradation and intermittent interference affecting GNSS receivers in specific geographic areas. In contrast, space-based RF sensing offers wide-area and often global coverage, enabling the detection of high-power or region-scale interference events that may affect large numbers of users simultaneously. While airborne and space-based systems are generally less sensitive to low-power emitters, they provide a strategic-scale perspective that complements terrestrial observations.

From a Defence perspective, integrating ground-based and space-based sensing enables PNT-SA across tactical, operational, and strategic timescales. Terrestrial systems can provide detailed local awareness and early warning in areas of interest, while space-based systems offer broader contextual awareness of interference patterns, persistence, and geographic extent. Together, these approaches support a layered perception capability that improves confidence in detecting contested PNT conditions across diverse operating environments. Within this perception layer, spectrum situational awareness can be supported through a range of implementation approaches, spanning open-source and community-driven resources through to integrated commercial systems.

4.1.1 Open Source Threat Intelligence Resources

Open-source and community-developed platforms play an important role in perception-level PNT situational awareness, particularly for experimentation, validation, and early-stage deployment of spectrum monitoring capabilities. Various open-source monitoring websites provide near real-time situational awareness of GNSS interference worldwide, drawing primarily on crowd-sourced data from ADS-B receivers. These platforms rely on the fact that aircraft continuously transmit position, velocity, and navigation status information, including indicators of GNSS signal health. By aggregating and analysing this data, they can identify regions where GPS signals appear degraded or unavailable, often as a result of jamming or spoofing.

Open-source aviation-derived interference monitoring platforms provide a valuable, low-cost input to PNT situational awareness by revealing large-scale and persistent patterns of GNSS disruption that may not be visible to individual users or operators. These platforms typically exploit aircraft ADS-B data, including reported position behaviour and associated integrity metrics such as the Navigation Integrity Category (NIC), to infer potential degradation in GNSS performance. While they rely on similar underlying data sources, the platforms differ in their aggregation methods, visualisation approaches, and analytical emphasis. Collectively, they illustrate how passive, crowdsourced aviation data can be exploited to detect, characterise, and contextualise GNSS interference activity across wide geographic areas. Some examples of such resources are shown in Table 18 below, noting that the list is not exhaustive, and other similar resources also exist.

Table 18: Examples of public domain threat intelligence resources.

Platform	Website	Primary Insight
GPSJam	https://gpsjam.org	Detection of GNSS interference inferred from aircraft position instability in ADS-B data.
GPSWise	https://gpswise.aero	ADS-B based detection of GNSS jamming and spoofing, through NIC degradation and anomalous position behaviour.
FlightRadar24	www.flightradar24.com/data/gps-jamming	Inference of GNSS interference using ADS-B-derived NIC degradation observed across multiple aircraft operating in close proximity.

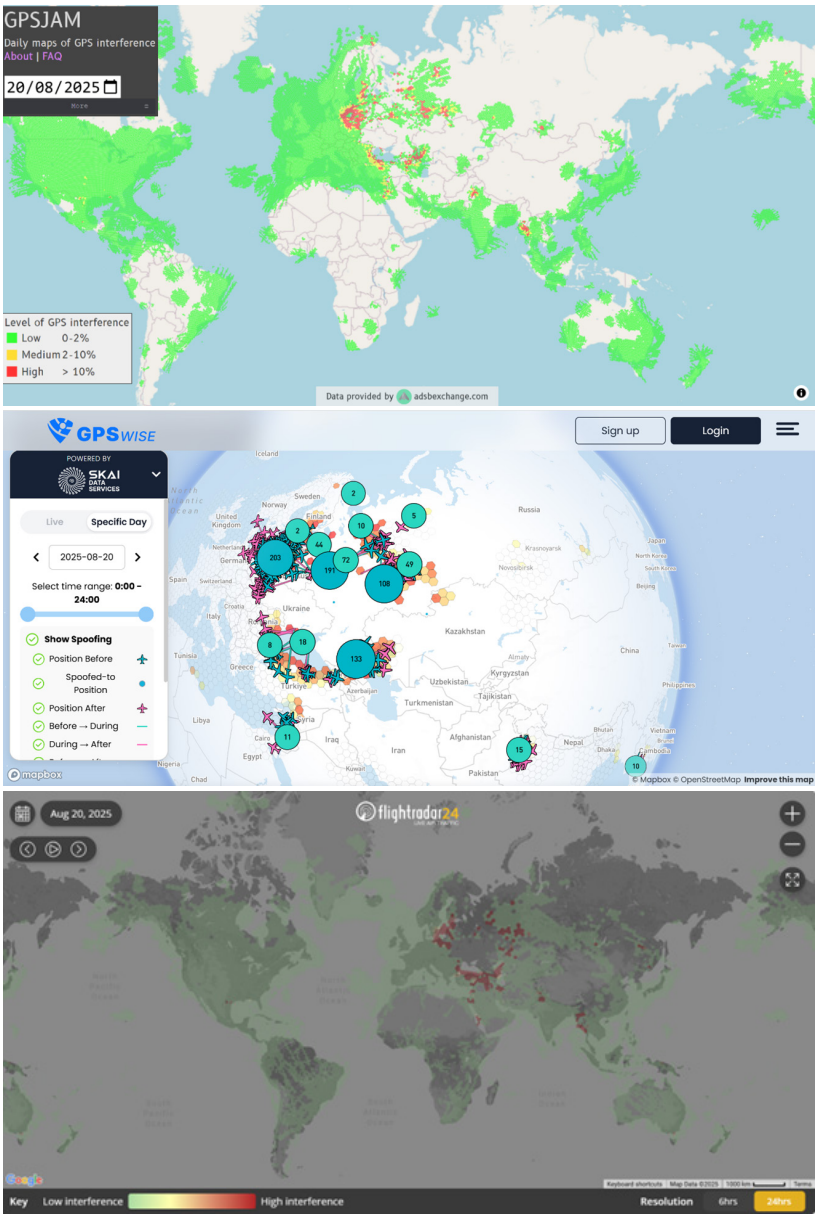

Figure 5 shows screenshots of the interfaces of these three resources taken from the same day on 20th August 2025 for a like-for-like comparison. Showing multiple platforms side-by-side highlights how similar underlying data can be interpreted and presented in different ways, reinforcing both the utility and the limitations of open-source interference intelligence for operational decision-making.

Figure 5: Comparison of public domain aviation GNSS interference monitoring interfaces.

4.1.2 Commercial Threat Intelligence Resources

In contrast, commercial platforms integrate these sensing and analysis functions into operationally deployable systems, offering greater scalability, reliability, and coverage for sustained monitoring. Table 19 presents representative examples of commercial and operational spectrum situational awareness solutions currently in use.

The examples illustrate the diversity of sensing architectures, coverage scales, and measurement approaches employed to support perception-level detection of GNSS and PNT interference. The list is not intended to be exhaustive, but rather to demonstrate the range of available methods used to establish awareness of anomalous RF activity affecting PNT services.

Table 19: Representative examples of commercial perception-level PNT-SA solutions.

System	Method	Coverage	Description
GPSat Systems GRIFFIN	Terrestrial multi-antenna array	Regional / national	Distributed network of synchronised sensor nodes using electronically steered phased array antennas to perform AOA, TDOA, FDOA, and PDOA measurements to detect interference over wide geographic areas.
HawkEye 360	Space-based RF sensing	Global (wide area RF)	LEO satellite clusters performing multi-satellite TDOA and FDOA analysis to detect, characterise, and geolocate RF emissions, including strong GNSS interference, over wide geographic areas.
GPS Patron Probe TGE2	Terrestrial GNSS interference monitoring station	Local / regional	Compact GNSS monitoring station capable of performing TDOA-based localisation, signal classification, and interference characterisation over local to regional areas.
UHU Technologies UHU1000	Terrestrial multi-antenna array	Local / regional	Ground-based GNSS threat detection system using multi-antenna arrays to detect, classify, and geolocate RF interference, including spoofing, at local to regional scales.
Oscilloquartz OSA5405	Terrestrial GNSS interference monitoring station	Local / regional	Compact GNSS monitoring and timing platform with integrated jamming and spoofing detection, supporting perception-level spectrum situational awareness at local to regional scales.
Aireon SWAM / IPV	Space-based ADS-B multilateration	Global (aviation)	Uses ADS-B signals received by multiple LEO satellites to perform TDOA-based multilateration for GPS-independent aircraft positioning and to validate or flag suspect GNSS-derived positions.
Spire GNSS Interference Detection	Space-based RF sensing	Global (wide area RF)	LEO satellite constellation detecting and analysing GNSS signal anomalies, combining ADS-B data and spectral measurements to identify and characterise interference events globally.
SeRo GRSD	Networked ADS-B and RF monitoring	Regional (airspace)	Real-time air-traffic overlay with GNSS RFI heatmap, AI-guided predictive alerts, and MLAT-based anomaly detection for jamming/spoofing surveillance.
Unseen Labs	Space-based RF sensing (AIS and non-cooperative maritime emissions)	Global (maritime)	LEO satellite constellation performing passive RF detection and geolocation of maritime transmitters, including AIS, to identify anomalous or non-cooperative vessel behaviour over wide oceanic areas.

Practical applications of PNT-SA range from monitoring air approaches at major airports and maritime navigation lanes at ports, to providing a wide area regional coverage. An example of regional coverage system is shown in Figure 6. This particular example shows the regional interference space tracking concept, where directional beams from three regional nodes (in yellow), and three TDOA intersect ellipse pairs (in purple) are used to detect interference coming from a LEO satellite.

Together, these perception-level capabilities provide the foundation for PNT-SA by enabling the early detection of anomalous RF conditions that may affect the reliability of GNSS and related PNT services. Currently the emphasis is on recognising that PNT conditions are degraded or contested, rather than on determining the precise source, intent, or implications of the interference. For Defence and other operators of safety-critical systems, this early awareness is essential for maintaining trust in PNT outputs and for triggering further analysis and response processes. The transition from detection to understanding, namely, determining what the interference is, where it originates, and how it is likely to affect operations, is addressed in the next layer of situational awareness, discussed in Section 4.2.

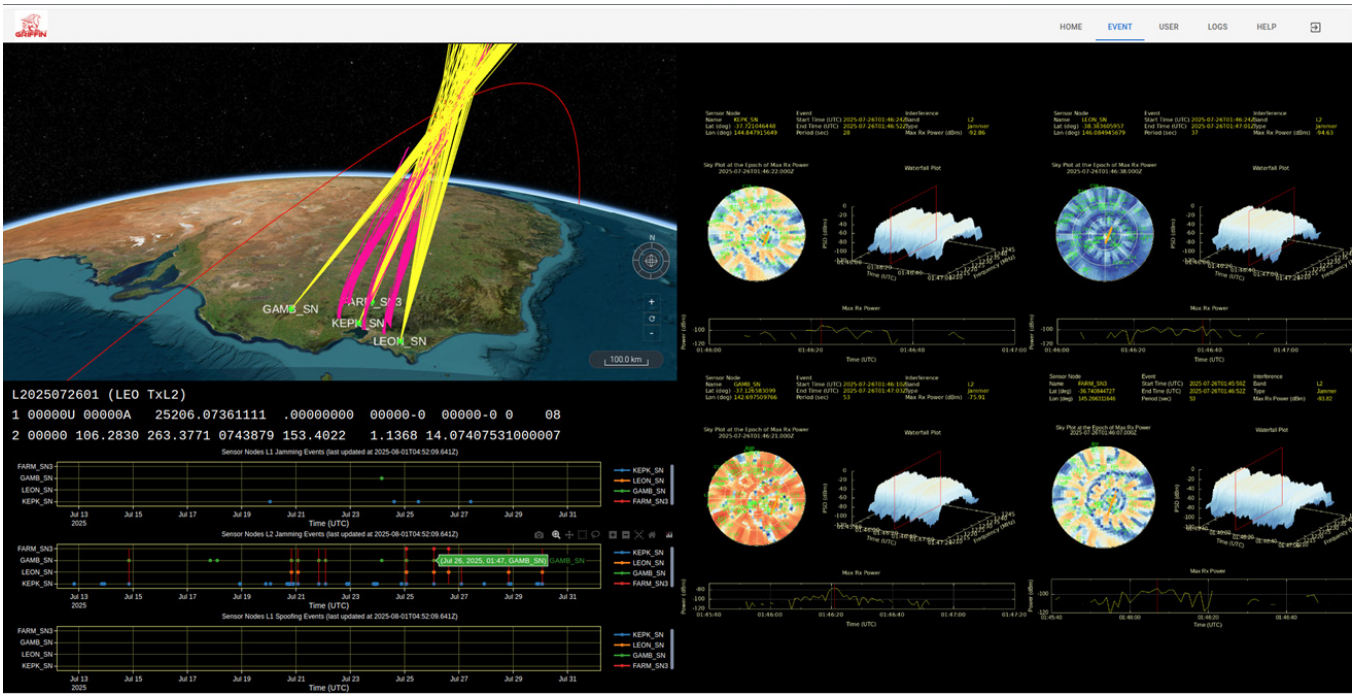

Figure 6: Example of a regional PNT-SA system (Source: https://gpsatsys.com.au/c7-activities).

4.2 Comprehension

At the comprehension level, PNT-SA moves beyond the detection of anomalous conditions to reducing uncertainty about the nature, location, and behaviour of interference to a level sufficient to support informed operational decision-making. Building on perception-level awareness that PNT conditions may be degraded or contested, comprehension seeks to determine what the interference is, where it originates, how it is evolving, and which users or systems are affected. This stage does not itself constitute response or mitigation; rather, it provides the contextual understanding required to assess severity, confidence, and potential impact before any action is considered. For Defence and other operators of safety-critical systems, comprehension is therefore the critical bridge between early warning and proportionate response, enabling informed judgement in complex and ambiguous operating environments.

4.2.1 Substantial Threat Localisation and Characterisation

High-confidence localisation typically fuses multiple complementary techniques to reduce ambiguity and improve confidence in emitter localisation and characterisation. While these techniques were introduced at a high level in the context of perception-level spectrum situational awareness, their role becomes more substantive at the comprehension stage, where they support emitter attribution, spatial discrimination, and confidence-weighted threat assessment. Table 20 summarises the key localisation and characterisation techniques commonly employed, highlighting their respective strengths, limitations, and operational applicability.

Table 20: Examples of threat localisation and characterisation techniques.

Technique	Description
AOA	Angle of Arrival uses electronically steered phased-array sensors to estimate the bearing to each emitter. With multiple sites, intersected bearings yield rapid 2D/3D fixes. Arrays also help separate co-channel threats and distinguish spoofers by their phase structure.
TDOA	Time Difference of Arrival uses precisely time-synchronised ground stations (or multi-sat clusters) to measure arrival-time to triangulate emitters. By intersecting the resulting hyperbolic curves from multiple receiver pairs, the location of the emitter can be triangulated. TDOA provides excellent geometry for locating stationary or slow-moving interference sources, such as fixed jammers.
FDOA	Frequency Difference of Arrival also uses precisely time-synchronised ground stations to measure Doppler differences in signals to triangulate emitters. FDOA is especially valuable for tracking moving interference sources, such as vehicle-mounted jammers or drones, where Doppler signatures help tighten the solution and distinguish mobile threats from static emitters.
PDOA	Power Difference of Arrival uses received-power gradients across the network to constrain range or refine the solution space. It is a useful technique when timing baselines are short or AOA geometry is poor, and as a check against multipath bias.
ADS-B	Automatic Dependent Surveillance-Broadcast data provide aircraft position and integrity indicators, with spatio-temporal clustering of integrity dropouts used to infer interference fronts and affected regions. Where dense ground sensing is unavailable, horizon-based methods use affected flight radio horizons to constrain jammer location to tens of kilometres, with refinement using contextual information.
AIS	Automatic Identification System data provide vessel position, identity, and transmission integrity indicators, with spatial and temporal anomalies used to infer GNSS interference or manipulation in the maritime domain. Aggregated AIS disruptions can reveal interference hotspots, spoofing, or non-cooperative behaviour, particularly in congested or strategically sensitive waterways.

Different techniques can be used by themselves or combined in a fused sensor array. Depending on the application, the system can be based on the ground, in the air and in space. Ground-based systems can be used at airports, marine ports, critical infrastructure sites and defence installations. They can provide local TDOA baselines, spectrograms, and GNSS observables such as signal-to-noise ratio (SNR) and code/carrier metrics to classify waveform type and quantify power/bandwidth. These instruments anchor the network with ground truth and speed on-scene refinement.

Air-based systems can use measurements from multiple LEO satellites to compute GNSS-independent position of the aircraft in real-time. These truth tracks can then be compared against the aircraft's own GNSS-derived positions, allowing spoofing impacts to be validated and the extent of the affected airspace to be mapped. This provides valuable insight into the scope and severity of spoofing events.

In practice, robust localisation fuses these methods – phased-array AOA for fast bearings; networked TDOA/FDOA (and, where helpful, PDOA) for precise 3D fixes; ADS-B analytics for area cues and continuity; multilateration for GPS-independent validation; and fixed probes for waveform and power characterisation. The outputs of these systems are not limited to coordinates, they include predicted impact maps over large areas.

4.2.2 Spectrum Policing & Interdiction

Detecting and localising interference is only part of the operational picture. Effective resilience also depends on the ability to respond to, and where possible remove, the source. Spectrum policing refers to the set of processes, tools, and authorities used to enforce lawful spectrum use, while mitigation encompasses technical and procedural measures to limit the impact of interference. For Defence operations, these response pathways must be integrated with existing command, control, and legal frameworks to ensure actions are timely, lawful, and proportionate. Once a source has been detected and geolocated, actionable intelligence is passed to enforcement agencies or site operators. The response may involve:

- **On-site investigation –** dispatching inspection teams equipped with portable direction-finding systems to visually confirm and disable the source
- **Remote intervention –** where infrastructure is accessible remotely, disabling transmitters via remote control or issuing a shutdown command to compliant devices.
- **Engagement with local authorities –** coordinating with police, spectrum regulators, or military units to secure the site and seize illegal equipment.

Spectrum policing effectiveness depends on clear jurisdiction, well-defined rules of engagement, and the ability to act quickly. In many countries, responsibility is shared between the national spectrum regulator, aviation and maritime authorities, and law enforcement.

Rapid action requires pre-arranged coordination protocols and, in some cases, international agreements, especially when interference crosses borders. A complete spectrum policing framework combines detection, localisation, characterisation, and enforcement into a continuous cycle. Lessons learned from each incident feed back into system tuning, procedural updates, and operator training, increasing resilience over time. Systems that integrate detection and localisation networks with incident management tools can reduce the time from first detection to on-scene neutralisation from days to hours, and in some cases, minutes.

4.3 Projection

In this report, Projection describes the forward-looking use of detected and localised interference information to anticipate where GNSS impacts are likely to occur under current conditions. It combines precise 3D geolocation of interference sources with electromagnetic propagation models to generate regional fog heat maps of RF power distribution, here referred to as Area of Interest Prediction (AOIP). These visualisations forecast the likely impact zones under current conditions of jamming or spoofing, showing not only where interference has been detected but also where its effects are expected to spread. Much like weather radar projecting storm cells and their trajectories, AOIP maps enable operators to foresee cascading impacts across aviation corridors, maritime approaches, and critical infrastructure nodes. Figure 7 shows an example of an AOIP heat map.

Geospatial visualisation tools play a key role in making these projections usable. Within a digital twin of an airport, maritime port, or logistics hub, AOIP overlays provide intuitive displays of where GNSS degradation is most likely to occur. This enhances decision-making by enabling early warnings to mission-critical users, informing the prioritisation and direction of enforcement activities, and supporting continuity planning for operators. Importantly, AOIP directly supports the Projection stage of situational awareness, underpinning resilience across response, recovery, and adaptation.

Together, these projection-level capabilities extend PNT-SA from understanding current interference conditions to anticipating their likely evolution in time and space. By combining detection and localisation outputs with propagation modelling and geospatial visualisation, operators gain foresight into where PNT degradation may emerge, persist, or intensify under prevailing conditions. While inherently probabilistic, this forward-looking awareness enables earlier warning, more informed prioritisation of response activities, and improved continuity planning for Defence and other operators of safety-critical systems. In this way, projection completes the situational awareness cycle by transforming technical understanding into actionable foresight that supports resilience across complex and dynamic operating environments.

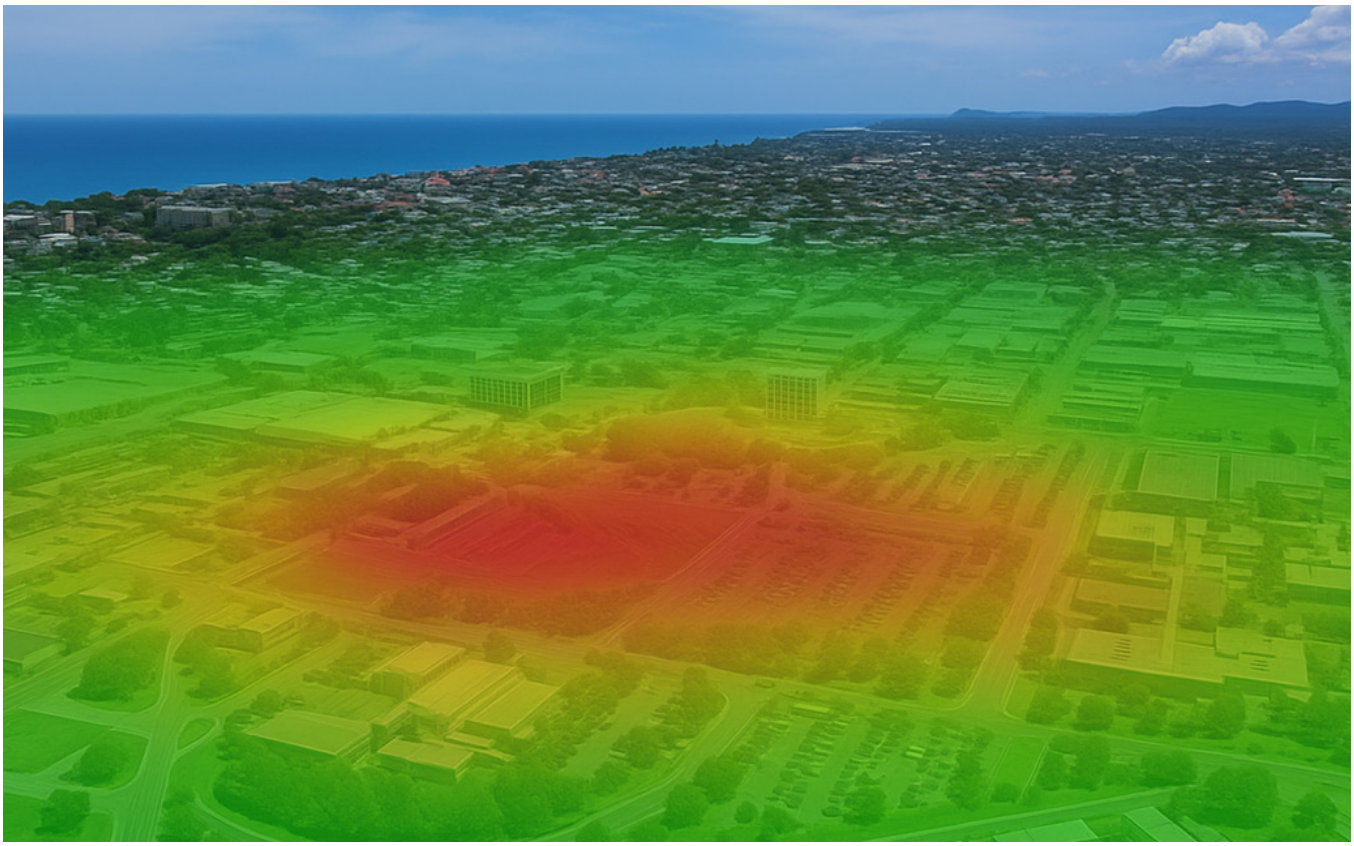

Figure 7: An example of an Area of Interest Prediction heat map.

4.4 Chapter Summary

This chapter examined PNT threat detection and response through the lens of situational awareness, framing resilience as a layered capability encompassing perception, comprehension, and projection. At the perception level, PNT-SA enables the early detection of anomalous RF conditions affecting GNSS and related PNT services, providing timely indication that PNT performance may be degraded or contested. Comprehension builds on this awareness by reducing uncertainty through threat localisation and characterisation, allowing operators to understand the nature, scale, and potential impact of interference with sufficient confidence to support informed decision-making. Projection extends this understanding forward in time and space, using modelling and visualisation techniques to anticipate how interference effects may evolve and propagate under prevailing conditions.

These layers transform PNT monitoring from a passive technical function into an operational decision-support capability. By linking detection, understanding, and foresight within a continuous cycle, situational awareness enables proportionate response, improved coordination, and more effective resilience planning across Defence and other safety-critical domains. The framework established in this chapter provides a foundation for considering how PNT threats translate into real-world impacts, and how resilience measures can be prioritised to reduce vulnerability and sustain trusted PNT in contested and complex operating environments.

For Australia and the broader Indo-Pacific region, PNT situational awareness is particularly relevant due to the scale of GNSS dependence across remote infrastructure, maritime and aviation operations, and critical timing applications. These applications combined with heightened exposure to space weather effects, interference risks, and limited redundancy in some regions further enhance this dependence.

By enabling early detection, informed interpretation, and forward-looking assessment of PNT disruptions, the approaches outlined in this chapter provide a practical foundation for enhancing PNT resilience. This foundation is especially important in geographically dispersed environments characterised by diverse threat vectors and growing reliance on satellite-based services.

For Defence, this situational awareness framework provides a basis for distinguishing nuisance interference from operationally significant threats, enabling proportionate responses, informed risk acceptance, and coordination across joint and coalition environments.

Chapter 5 provides an extensive overview of the resilient PNT technology landscape, examining the strengths, limitations, and maturity of key space-based, terrestrial, and onboard capabilities.

5 PNT CAPABILITY ARCHITECTURES AND ENABLING TECHNOLOGIES

GNSS has long served as the primary source of PNT information for most civil and defence applications, and it continues to underpin the majority of PNT use cases today [48]. However, increasing awareness of GNSS vulnerabilities, particularly to jamming, spoofing, space weather, and systemic failures, has highlighted the risks of relying on a single dominant technology for critical services. Some of these methods are outlined in Chapter 4, with this Chapter acting as a bridge to ensuring continuous capability in a degraded and denied environment.

In response to this threat, governments and industry are increasingly investing in a broader range of PNT technologies designed to complement GNSS and support operations in such environments. These efforts reflect a shift away from single-system dependency towards diversified PNT capability architectures, in which different technologies provide complementary or alternative functions depending on the operational context.

This chapter reviews the principal technology classes that contribute to a modern PNT capability. These include space-based systems beyond traditional GNSS, terrestrial broadcast systems, timing resilience technologies, and onboard navigation solutions that do not rely on any external radionavigation signals. Together, these technologies form the technical basis for more resilient PNT across Defence and critical infrastructure sectors.

Summaries of selected technology test campaigns and evaluation programmes from the United States and the European Union are provided in Appendix B.

The discussion begins with satellite-based PNT, reflecting its continuing role as the foundational layer in most contemporary PNT capability architectures.

5.1 Multi-layered Satellite PNT Architectures

Satellite-based PNT is, and is likely to remain, the foundation layer of most PNT capability architectures in the foreseeable future [50]. However, it should not be viewed as a single, homogeneous capability. Instead, future development comprises multiple orbital layers, each with distinct characteristics in terms of signal geometry, coverage, latency, power, and resilience.

These layers span Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary and geosynchronous orbits (GEO), and they fulfil different functional roles within PNT architectures. MEO constellations underpin GNSS, providing worldwide positioning and timing services. Geostationary and inclined geosynchronous orbits are typically used to support augmentation and regional navigation services, while emerging LEO constellations offer alternative signal characteristics that complement traditional GNSS performance, as well as permitting new innovations in terms of cost and agility to orbit.

Understanding satellite-based PNT as a multi-layered architectural domain, rather than a single technology class, is essential for evaluating how satellite systems contribute to resilient PNT solutions. The remainder of this section examines the principal satellite-based services and orbital regimes that form this layered architecture, before later sections consider how satellite PNT is complemented by terrestrial, timing, and onboard technologies.

5.1.1 Global and Regional Satellite Navigation Systems

GNSS represents the most mature and widely deployed implementation of satellite-based PNT, forming the core of the MEO layer within contemporary PNT capability architectures. These systems provide global services and underpin the majority of civil, commercial, and defence PNT applications worldwide.

At present, four fully operational global GNSS constellations are in service – GPS operated by the United States, GLONASS operated by the Russian Federation, Galileo operated by the European Union, and BeiDou operated by China. Each constellation comprises a network of satellites, primarily in MEO, broadcasting ranging and timing signals to enable user position and time estimation.

In addition to global systems, several regional navigation satellite systems (RNSS) provide enhanced coverage or performance over specific geographic areas. These systems typically employ inclined geosynchronous or highly elliptical orbits to increase satellite availability and geometry over their regions of interest. Examples include Quasi-Zenith Satellite System (QZSS) operated by Japan, Navigation with Indian Constellation (NavIC) operated by India, and the emerging Korean Positioning System (KPS) being developed by the Republic of Korea. While regional in scope, such systems can significantly improve performance and robustness for users within their coverage areas.

Although the availability of multiple global and regional constellations has increased redundancy at the signal level, GNSS collectively share common architectural characteristics. They operate in similar orbital regimes, rely on comparable signal structures, and predominantly occupy the L-band radiofrequency spectrum. Coordination on signal design, spectrum use, and interoperability take place under international frameworks such as the United Nations International Committee on GNSS (UN ICG) and the International Telecommunication Union (ITU). As a result, multi-constellation GNSS usage improves availability, geometry and interoperability under nominal conditions, but does not, on its own, eliminate systemic vulnerabilities to interference, spoofing, or space-environment effects.

For these reasons, GNSS should be understood as a critical, but not sufficient by itself, component of resilient PNT capability architectures. Subsequent sections therefore examine how GNSS is being augmented, modernised, and complemented by other satellite layers and non-satellite technologies to address these limitations.

5.1.1.1 Frequency Congestion and Architectural Constraints

Despite the increasing number of global and regional GNSS constellations, satellite-based navigation systems share a common and increasingly congested RF environment. Most GNSS signals are transmitted within the L-band, which offers favourable propagation characteristics for space-to-Earth links, but provides limited spectrum for simultaneous, globally interoperable services.

As additional constellations, signals, and services have been introduced, the L-band environment has become progressively more crowded. This has increased the complexity of signal co-existence, receiver design, and interference management, particularly in environments where GNSS signals are already weak relative to local RF noise. While modern receivers are capable of tracking multiple constellations and signals concurrently, they remain fundamentally constrained by the shared spectral and power characteristics of GNSS transmissions.

From an architectural perspective, this shared spectrum represents a common mode of vulnerability across GNSS implementations. Multi-constellation operation improves availability and geometry under nominal conditions, but it does not eliminate susceptibility to wideband interference, jamming, or other disruptions affecting the L-band as a whole. Consequently, increasing the number of GNSS signals alone does not provide true architectural diversity.

These constraints highlight an inherent limitation of relying exclusively on GNSS-based solutions for resilient PNT. While continued GNSS modernisation can improve performance, authentication, and integrity within the satellite layer, addressing systemic vulnerabilities requires diversification beyond a single frequency band and orbital regime. This consideration underpins growing interest in complementary satellite layers and non-satellite PNT technologies, which are examined in subsequent sections of this chapter.

5.1.1.2 GNSS Modernisation Initiatives

Ongoing modernisation programmes across global and regional GNSS constellations aim to enhance performance, service assurance, and robustness within the existing satellite navigation paradigm. These initiatives focus on improving signal structures, power levels, integrity monitoring, and authentication, while maintaining backward compatibility with legacy receivers and services.

In the United States, the deployment of GPS III and the planned GPS IIIF satellites represent the most significant evolution of GPS since its initial operational capability. These satellites introduce higher signal power, improved clocks, and enhanced civil signals, including the L1C signal designed for interoperability with other constellations [51]. A key development within this modernisation effort is the introduction of civil signal authentication through Chips Message Robust Authentication (CHIMERA), which enables users to verify the authenticity of navigation messages and provides protection against certain spoofing scenarios [52].

The European Union's Galileo programme has similarly prioritised service assurance through the implementation of Open Service Navigation Message Authentication, known as OSNMA [53]. OSNMA allows receivers to authenticate navigation data without restricting access to authorised users, improving trust in Galileo signals while preserving its open-service model. Comparable modernisation efforts are underway across other GNSS constellations, including enhancements to signal structures, clock performance, and system monitoring.

Other GNSS providers, including Russia and China, are also pursuing modernisation initiatives focused on improved signal structures, constellation management, and service performance, broadly aligned with the global trend towards enhanced robustness within the GNSS layer [54, 55].

While these developments represent meaningful advances in GNSS capability, they do not fundamentally alter the architectural characteristics of the GNSS layer. Modernised systems remain reliant on MEO satellites broadcasting low-power signals in the L-band, and therefore continue to share common-mode vulnerabilities associated with spectrum congestion, interference, and space-environment effects. GNSS modernisation should therefore be viewed as evolutionary improvement within a single architectural layer, rather than a substitute for broader PNT diversification.

Separately, experimental and demonstration programmes such as the United States Space Force's Navigation Technology Satellite-3 (NTS-3) are exploring more flexible signal generation, reprogrammable payloads, and adaptive concepts for future navigation satellites. While promising, these efforts remain at the experimental stage and are not yet indicative of near-term changes to operational GNSS architectures [56].

5.1.1.3 Satellite Based Augmentation Systems

Satellite-Based Augmentation Systems (SBAS) extend GNSS performance by providing regional corrections, integrity monitoring, and availability enhancements, through geostationary satellite platforms. SBAS services are widely used in safety-critical applications, particularly in aviation, where integrity and continuity requirements exceed those of standard GNSS services [57].

From an architectural perspective, SBAS represents an augmentation of the GNSS layer rather than an independent PNT capability. While SBAS can improve accuracy and integrity within its coverage area, it remains dependent on GNSS signals and shares many of the same common-mode vulnerabilities associated with satellite-based navigation, including susceptibility to interference affecting the underlying GNSS signals. The map of current operational and planned systems is shown in Figure 8 below.

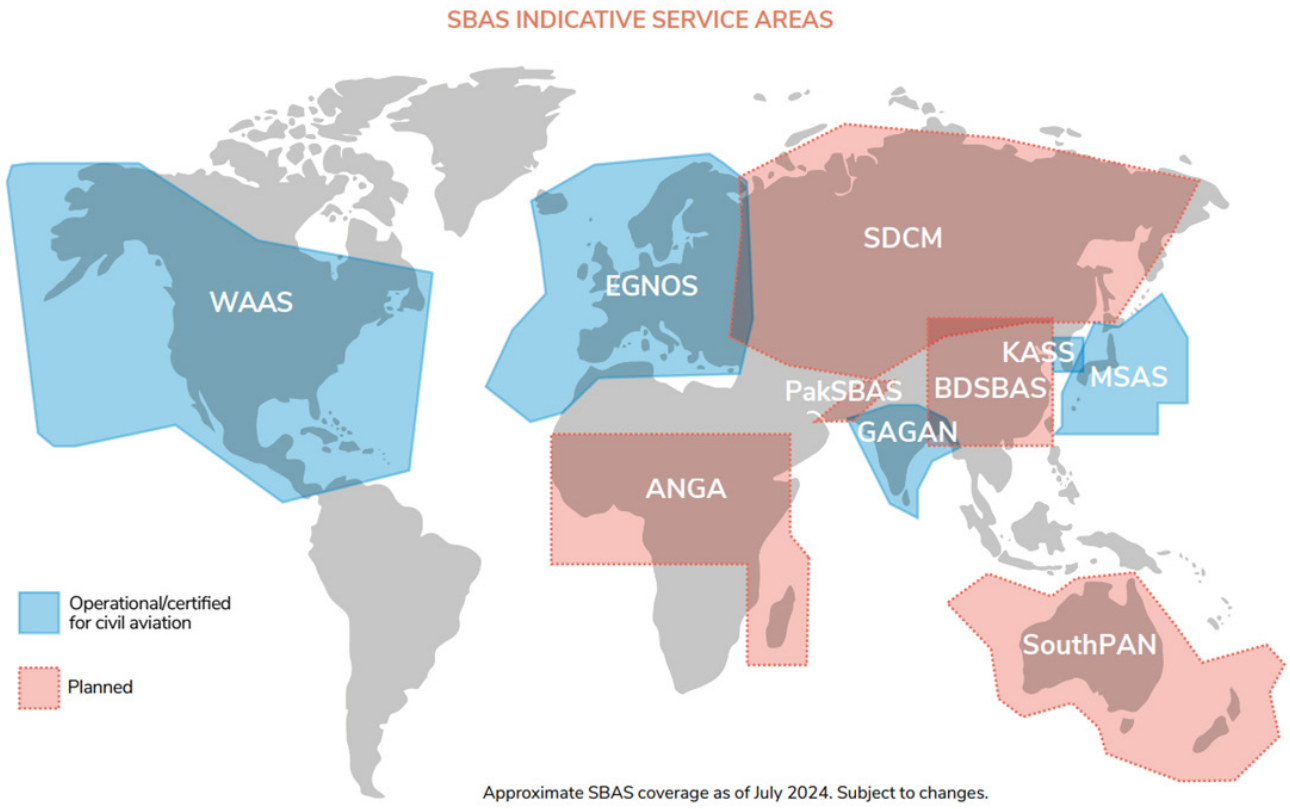

Figure 8: Map of currently operational and planned SBAS services [58].

5.1.2 LEO PNT

LEO satellite systems are increasingly being explored as a complementary layer within multi-layered PNT capability architectures. Operating at altitudes of between 500 km and 2,000 km, LEO satellites exhibit fundamentally different characteristics to traditional MEO GNSS constellations, with implications for signal strength, geometry, latency, and resilience.

From an architectural perspective, the most significant distinction of LEO-based PNT is the substantially reduced satellite-to-user range, which enables higher received signal power and faster signal dynamics. These properties can improve robustness against certain interference scenarios and enable more rapid geometry changes, potentially benefiting positioning performance in challenging environments such as urban canyons, high-latitude regions, and areas with partial sky visibility [59].

A further distinguishing feature of LEO-based PNT architectures is the potential for greater frequency diversity. Whereas GNSS services are almost exclusively confined to the L-band, many LEO PNT concepts operate, or propose to operate, across a broader range of frequency bands, including S-band, C-band, and higher frequencies associated with modern communications payloads. This has been possible with a reduced cost to manufacture and launch to LEO, allowing services to adapt to changing technology and frequency conditions. The diversity enables PNT signals to be distributed across different spectral environments with distinct propagation, interference, and congestion characteristics [59].

From an architectural perspective, frequency diversity provides an additional dimension of resilience that cannot be achieved through multi-constellation GNSS alone. By reducing dependence on a single frequency band, LEO-based PNT systems may mitigate certain common-mode vulnerabilities affecting L-band services, particularly in environments where interference or congestion is concentrated within GNSS frequencies.

However, the use of higher-frequency bands also introduces trade-offs related to propagation loss, susceptibility to obstruction, and regulatory coordination. LEO constellations require significantly larger numbers of satellites to achieve continuous global coverage, introduce higher Doppler dynamics, and depend on frequent satellite handovers. As a result, LEO-based PNT systems are inherently more complex to design, deploy, and operate than traditional GNSS constellations.

Importantly, LEO PNT should not be viewed as a direct replacement for GNSS. Instead, it represents a complementary satellite layer that may enhance overall PNT resilience when integrated with existing MEO-based systems and non-satellite technologies. The value of LEO PNT therefore lies not in replacing GNSS, but in providing architectural diversity through different orbital regimes, signal characteristics, and deployment models.

The following subsections examine the principal approaches to LEO-based PNT, including dedicated navigation constellations, signals of opportunity derived from communications systems, and experimental and demonstration programmes. Their maturity, performance characteristics, and potential roles within resilient PNT architectures are considered in the context of the broader technology landscape outlined in this chapter.

5.1.2.1 Dedicated LEO PNT Constellations

Dedicated LEO PNT constellations are systems explicitly designed to deliver PNT services as a primary mission, rather than deriving PNT as a secondary function of communications or sensing payloads. These constellations typically employ purpose-built navigation payloads, tailored orbit configurations, and system architectures optimised for PNT performance and service assurance.

A number of dedicated LEO PNT concepts are currently under development, with varying levels of maturity and intended application. Table 21 provides an overview of selected dedicated LEO PNT initiatives, including indicative constellation sizes, deployment status, and frequency bands where publicly available information exists [59]. Iridium PNT is the only operational service delivering PNT from LEO, while most other initiatives remain in early development or initial deployment phases. As such, many of these systems are several years away from initial operating capability, and further still from full operational maturity.

Table 21: Dedicated LEO PNT Constellations [59].

Organisation	Country of Origin	Government / Private	No of Sats (Planned)	No of Sats (Launched)	Frequency Band
Iridium PNT	USA	Private	66	66	L
Xona Space	USA	Private	258	1	L
TrustPoint	USA	Private	300	1	C
JAXA	Japan	Government	480	0	C
ArkEdge Space	Japan	Private	~300	0	VHF, L, S, C
Centispace	China	Private	190	unknown	L
Geely	China	Private	240	unknown	L
SatNet LEO	China	Government	506	unknown	L
Celeste IoD	Europe	Government	10	0	L, S, C, UHF

Additionally, several other countries including Türkiye, the United Arab Emirates, South Korea, Russia, and India have publicly expressed interest in developing dedicated LEO PNT capabilities through international forums such as the International Committee on GNSS (ICG), however at the time of writing, limited technical or programme-level detail is available for these initiatives.

While differing in implementation, these efforts share a common objective of complementing GNSS by providing alternative signal geometries, higher received power, and architectural diversity.

From an architectural perspective, dedicated LEO PNT constellations offer several potential advantages relative to traditional GNSS. Reduced satellite-to-user range enables stronger signals at the receiver end, which may improve robustness in environments affected by attenuation and signal obstruction, as well as providing stronger resilience to jamming. Rapid satellite motion can also enhance geometric diversity over short timescales, potentially benefiting positioning performance in dynamic or constrained environments.

As a result, dedicated LEO PNT constellations should be viewed as an emerging complementary capability, rather than a near-term replacement for GNSS. Their potential contribution to resilient PNT architectures lies in their ability to introduce both orbital and spectral diversity, augmenting existing GNSS technologies in use-case-specific deployments.

5.1.2.2 LEO Signals of Opportunity

Signals of Opportunity (SoOP) refer to the use of existing RF transmissions, not originally designed for navigation, to support PNT applications. In the context of LEO, SoOP approaches typically leverage signals transmitted by large satellite communication (SATCOM) constellations, exploiting their signal structure, geometry, and global coverage to derive PNT information without deploying dedicated navigation payloads.

Several LEO SATCOM systems have attracted interest as potential SoOP sources for PNT, including constellations such as Starlink, OneWeb, Amazon LEO, and other emerging broadband satellite networks [60]. These systems transmit high-power signals across a range of frequency bands and operate dense constellations with rapid satellite motion, creating favourable conditions for ranging, Doppler-based positioning, and time transfer techniques under certain assumptions.

From an architectural perspective, LEO SoOP approaches offer several potential advantages. Because the signals are already deployed for commercial SATCOM purposes, SoOP-based PNT can, in principle, be realised without the cost and complexity of launching dedicated navigation constellations. The use of diverse frequency bands and signal structures also introduces a degree of spectral diversity relative to traditional GNSS, which may be beneficial in environments affected by interference concentrated in the L-band.

However, LEO SoOP approaches are subject to significant limitations. Because the signals are not designed for PNT, their structure, timing stability, and availability are not ideal to deliver high performance. In addition, as access to signal specifications, precise timing references, and system metadata may be restricted or subject to change at the discretion of the constellation operator. As a result, SoOP-based PNT performance and reliability can be highly dependent on commercial, regulatory, and governance factors beyond the control of the end user.

Furthermore, SoOP techniques typically require sophisticated signal processing, calibration, and integration with other sensors, or PNT sources, to achieve useful performance. This limits their applicability as standalone solutions and reinforces their role as a complementary capability within hybrid PNT architectures. Consequently, LEO signals of opportunity should be viewed as a potentially valuable, but opportunistic component of resilient PNT architectures. Their primary contribution lies in enabling additional layers of diversity and redundancy when integrated with GNSS, dedicated LEO PNT services, terrestrial systems, and onboard sensors, rather than in providing an assured, independently governed PNT service in their own right.

5.1.2.3 Fused SATCOM-PNT Programmes

Fused SATCOM-PNT programmes represent an emerging approach in which PNT functionality is deliberately integrated into satellite communications systems, rather than delivered as a standalone navigation service, or derived opportunistically from existing signals. In these architectures, communications and PNT are treated as co-designed functions, sharing satellite platforms, waveforms, and ground infrastructure, with PNT performance considered explicitly at the system level [58].

A key enabler for such approaches is the development of 5G Non-Terrestrial Networks (5G-NTN), defined within standards developed by the 3rd Generation Partnership Project (3GPP), the international collaboration responsible for specifying global cellular communications technologies including 4G LTE and 5G [61]. Within the 3GPP framework, NTN waveforms, reference signals, and timing structures are standardised to support mobility, synchronisation, and positioning functions across satellite and terrestrial segments. This creates the technical foundation for extracting time and range observables from satellite communications signals in a controlled and interoperable manner, rather than through ad-hoc signal exploitation.

From an architectural perspective, fused SATCOM-PNT systems differ fundamentally from LEO signals-of-opportunity approaches. While both may leverage communications waveforms, fused systems assume operator cooperation and intentional design, including access to signal specifications, timing references, and system metadata. This enables tighter control over PNT performance, potential service definition, and more predictable behaviour than is possible with purely opportunistic techniques. However, unlike dedicated navigation constellations, fused systems typically prioritise communications performance, with PNT delivered as an integrated, but secondary capability.

Several international initiatives are now exploring fused SATCOM-PNT concepts within this framework. In Europe, for example, the IRIS² programme has been identified as a potential platform for assessing PNT capabilities derived from 5G-NTN satellite communications signals [62]. In this context, PNT is not delivered through dedicated navigation payloads, but through the exploitation of standardised communications signals combined with operator-provided timing and orbital information. Similar concepts are being explored elsewhere through research programmes, defence-led studies, and industry-driven demonstrations aligned with next-generation satellite communications architectures.

Despite growing interest, fused SATCOM-PNT programmes remain at an early stage of maturity. To date, no fused system has demonstrated the service assurance, governance arrangements, and long-term stability required for operational PNT delivery in safety-critical applications. Key challenges include dependence on communications network design choices, spectrum and regulatory constraints, evolving standards, and the need to reconcile commercial service priorities with PNT performance and continuity requirements.

Accordingly, fused SATCOM-PNT should be viewed as a promising, but exploratory architectural direction, rather than as an established PNT technology class. Its potential contribution lies in introducing additional orbital, spectral, and infrastructural diversity within multi-layered PNT architectures, particularly where integration with future communications networks is desirable. Further evaluation and demonstration will be required before such systems can be considered viable complements to existing satellite and non-satellite PNT capabilities.

5.1.3 Hybrid Multi-Orbit PNT Services

Hybrid satellite PNT approaches seek to improve resilience by combining multiple orbital regimes, including LEO, MEO and GEO, rather than relying on a single satellite layer. Architecturally, the motivation is two-fold. First, different orbit classes offer complementary geometry and coverage characteristics. Second, hybrid concepts often enable frequency diversity by leveraging non-GNSS transmissions across Ku/Ka/C (and other) bands, thereby reducing dependence on the congested GNSS L-band [63].

A related and increasingly visible trend is the emergence of PNT-as-a-Service models, where PNT capability is delivered via a service layer that supports navigation using non-PNT waveforms (most commonly commercial SATCOM transmissions used as signals of opportunity) [64]. In this model, the operator (or a third-party service provider) deploys monitoring and processing infrastructure that receives and characterises available signals, then distributes the information required for user equipment to form pseudorange-like observables. In practical terms, this model is often presented as a near-term resilience overlay that can support timing and positioning in GNSS-degraded conditions by leveraging existing commercial satellite infrastructure and additional ground/service components.

From a resilience perspective, these hybrid and service-layer approaches are attractive because they can introduce orbital diversity, frequency diversity, and delivery-model diversity. However, they also introduce new dependencies and design trade-offs that must be acknowledged. The approach relies on additional infrastructure (monitoring networks, data distribution, and associated governance), and on sufficient knowledge of signal characteristics and satellite states to enable stable ranging. The user segment may also face constraints depending on the bands exploited (e.g., antenna considerations, blockage sensitivity at higher frequencies, and receiver complexity). Hybrid multi-orbit and PNT-as-a-service concepts are best understood and leveraged in the context of a broad multi-layered PNT architecture, particularly where tailored resilience solutions are required for critical users or regions.

5.1.4 VHF Data Exchange System Ranging Mode (VDES-R Mode)

The VHF Data Exchange System (VDES) is an emerging maritime communication framework that builds upon the legacy Automatic Identification System (AIS) and is designed to operate across both terrestrial and satellite links. Operating in the maritime VHF band, VDES supports two-way digital data exchange between vessels, shore infrastructure, and satellites. Compared to AIS, VDES significantly increases data capacity and enables a broader range of safety, traffic management, and navigation-related applications.

It is important to note that VDES comprises both space-based and terrestrial components, with the terrestrial VDES network forming the primary operational backbone for safety-critical maritime services [65]. This section focuses on the satellite-based component of VDES in the context of R-Mode, while Section 5.2.2.2 provides further detail on the terrestrial implementation of VDES.

A notable extension of VDES is Ranging Mode (R-Mode), which introduces the capability to support positioning and timing functions as a complementary or backup PNT source for maritime users. In this mode, VDES shore stations and satellites transmit time-referenced signals that can be used by receivers to derive position estimates using time of arrival or time difference of arrival techniques. Because these signals are transmitted from known locations and operate in a frequency band distinct from GNSS, VDES R-Mode offers an additional layer of resilience in coastal waters, congested ports, and other GNSS-challenged maritime environments [66].

From an architectural perspective, VDES occupies a hybrid position between satellite-based and terrestrial broadcast PNT technologies. While the system includes a satellite communications component, current R-Mode concepts are primarily focused on terrestrial VHF infrastructure, with satellite links viewed as a potential future extension rather than a fully realised navigation service. As such, VDES R-Mode is best understood as a domain-specific PNT capability, rather than a global alternative to GNSS.

Standardisation and governance of VDES are being coordinated through the International Telecommunication Union (ITU) and the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), with multiple trials and pilot deployments underway internationally.

As part of the current standardisation process, the use of VDES for navigation is constrained by its spectrum allocation within the maritime VHF band. Under existing ITU arrangements, VDES is allocated primarily as a communications service and holds a secondary spectrum status, which limits available bandwidth and means that VDES transmissions must not cause harmful interference to primary services and cannot claim protection from them. As a result, VDES R-Mode is not presently suitable for designation as a Safety-of-Life (SoL) navigation service, as signal availability and interference conditions cannot be guaranteed, particularly outside controlled maritime environments.

Some regions of the world under the ITU have denied use of the VDES satellite sourced signals, including China, Vietnam, South Korea and Russia, which can restrict use over certain regions. However, for the case of Australia, it can be freely used, and alongside a targeted strategy for implementation, it can provide an alternative form of navigation.

Despite these limitations, VDES-R Mode represents a credible and operationally grounded resilience measure for the maritime sector. In Australia, for example, the Australian Maritime Safety Authority (AMSA) has highlighted the potential role of VDES and R-Mode within its Navigation Services 2035 outlook, particularly as part of a layered approach to maritime navigation resilience [67].

5.2 Terrestrial Broadcast

Terrestrial broadcast PNT systems offer a practical complement to satellite-based services by providing signals from ground infrastructure with different propagation characteristics, operating constraints, and threat profiles. This section summarises the principal terrestrial broadcast and terrestrial ranging approaches in use internationally, ranging from wide-area low-frequency services and coastal R-Mode implementations to local-area pseudolite networks and emerging broadcast-based positioning concepts. The discussion is descriptive, focusing on underlying principles, indicative performance, and deployment status. Considerations for Australian prioritisation and implementation pathways are addressed in Chapter 6.

While terrestrial broadcast PNT systems can provide backup to GNSS, they also introduce their own dependencies and risks, including transmitter availability, spectrum management, and the need to maintain consistent service performance through governance, monitoring, and ongoing maintenance of the underlying terrestrial infrastructure.

The technologies covered span several distinct *coverage classes*. eLoran represents the best-known example of a wide-area terrestrial service, using high-power low-frequency transmissions that can support robust timing and regional positioning. R-Mode leverages existing maritime radio infrastructure, such as Medium Frequency (MF) beacons and VHF AIS/VDES to provide an independent ranging capability in coastal waters. Local-area terrestrial ranging networks (often described as pseudolite approaches) target high-accuracy positioning within ports, industrial sites, or other defined operational areas. Finally, cellular and broadcast-based methods, such as 5G positioning and emerging broadcast positioning concepts, illustrate how resilience capabilities may also be realised by re-using mass-market communications networks.

5.2.1 eLoran

Enhanced Loran (eLoran) is a modernised form of the long-running Loran terrestrial radionavigation system, designed to provide an independent positioning and timing reference using high-power, low-frequency ground transmissions. Unlike satellite signals, eLoran relies on a network of fixed transmitters and groundwave propagation, allowing coverage to extend hundreds of kilometres and offering comparatively good penetration into some built and coastal environments. In most contemporary concepts, eLoran is positioned primarily as a timing and resilience service (with positioning as a secondary capability), providing a GNSS-independent reference that can be integrated into a layered PNT architecture.

From a user perspective, eLoran positioning is based on measuring the signal travel time from multiple transmitters and combining those measurements to estimate range. For timing users, eLoran can deliver an UTC-traceable time reference when transmitters are disciplined to a common time source and the service is operated with appropriate monitoring and control. A key attraction of eLoran in resilience discussions is that it presents a different set of vulnerabilities to GNSS, namely high transmitted power and long wavelength change the interference physics and can raise the effort required for wide-area disruption compared with weak satellite signals.

Achieving useful positioning performance also requires accounting for location-dependent propagation delays. Over land and coastal regions, variations in ground conductivity and terrain can introduce additional delays beyond a simple *speed of light* travel-time model. These effects are commonly addressed using Additional Secondary Factor (ASF) corrections derived from surveys and service-area characterisation, typically represented as ASF maps or models that can be applied by receivers. As a result, eLoran performance is highly dependent on system design and operational implementation, including transmitter geometry, calibration effort, monitoring, and the extent to which ASF modelling is maintained over time. Table 22 shows some general characteristics of eLoran performance.

Table 22: eLoran performance metrics.

Performance Metric	Value
Positional Accuracy	8-10 m (95%) – Maritime 10-20m – Land and mixed terrain [68]
Timing Accuracy	50 nanoseconds of UTC [69]
	Japan
Coverage	1600km – Timing and Data 1300km – Positioning Enhanced over saltwater paths [70]

Recent moves by several nations show renewed momentum behind eLoran as a sovereign, terrestrial complement to GNSS for both navigation and precise timing. Table 23 lists the current eLoran installations around the world.

Table 23: eLoran installations around the world.

Country	Status	Number of Stations	Motivation / Driver
South Korea	Operational (expanding)	5 transmitters + 43 differential sites	Persistent GNSS jamming from neighbouring regions; need for sovereign backup [71].
United Kingdom	Operational (expanding)	1 active transmitter; expansion to 6 sites funded	National PNT resilience strategy following 2017 Blackett Review [72, 73].
China	Operational	10 transmitters	Strategic redundancy to BeiDou; military navigation resilience [74].
Saudi Arabia	Operational (modernised)	Not disclosed	Sovereign infrastructure needs [75].
Russia	Operational (Chayka)	14 transmitters	Sovereign nav/timing; Arctic & maritime coverage [76].

5.2.2 Terrestrial Ranging Mode (R-mode)

Terrestrial R-Mode is a family of emerging terrestrial navigation technologies intended to provide independent and resilient PNT capability, particularly for the maritime domain. R-Mode re-uses existing radio communication infrastructure, such as MF differential GNSS (DGNSS) beacons and VHF AIS/VDES networks, to transmit precisely timed ranging signals that allow receivers to determine their distance from multiple transmitters using time or phase-based measurements. By exploiting infrastructure already in place for maritime safety and communication, terrestrial R-Mode offers a potentially cost-effective, GNSS-independent PNT layer that is intended to remain available during satellite disruption.

5.2.2.1 MF R-Mode

MF R-Mode is a terrestrial navigation technology designed to provide resilient position and timing services in coastal and inland waterways. It operates in the 285-325 kHz maritime MF band, re-using the infrastructure of existing radio navigation beacons and DGNSS stations. By embedding precisely timed ranging signals into the transmission of these beacons, MF R-Mode provides an independent PNT capability that can continue functioning when GNSS is unavailable or degraded.

In MF R-Mode, shore-based transmitters broadcast continuous, phase-stable signals from fixed, surveyed locations. Ships equipped with compatible receivers can measure the signal's time of arrival or phase relative to a known reference to determine position, typically by trilateration between multiple stations. Because MF signals propagate as ground waves over seawater with relatively low attenuation, coverage distances of up to ~300 km from the coast have been demonstrated, making MF R-Mode well-suited for navigation in coastal shipping lanes and harbour approaches [77].

Operating at lower frequencies than GNSS, MF R-Mode exhibits different interference characteristics and can raise the difficulty of disruption using techniques optimised for satellite signals. MF R-Mode can also support timing applications by providing a stable terrestrial time reference, typically synchronised to UTC via GNSS or other sources and then maintained locally during GNSS outages, with achievable performance dependent on system design and operational configuration.

5.2.2.2 VHF R-Mode (AIS/VDES)

A second implementation of R-Mode uses the VHF maritime band (156-162 MHz), extending the concept to communication systems already mandated on most vessels. Early prototypes, commonly referred to as AIS R-Mode, embed ranging bursts within existing AIS time slots. Subsequent development within the VDES standard introduces dedicated ranging channels with improved synchronisation, higher bandwidth, and compatibility with future space-based VDES services. These approaches are collectively referred to as VHF R-Mode, as they share the same fundamental ranging principle.

Demonstrations conducted under the R-Mode Baltic Project and by the U.S. Department of Transportation (DOT) have validated the technical feasibility of VHF R-Mode, achieving positioning accuracies on the order of 10 m and reliable operation to distances of approximately 150 km from shore, particularly when combined with MF R-Mode [78, 79]. Because VHF R-Mode can be transmitted using existing AIS base stations or upgraded VDES infrastructure, it represents a pragmatic pathway toward regional resilient PNT coverage.

5.2.2.3 Resilience and Integration Potential

Terrestrial R-Mode technologies are explicitly designed to complement GNSS by providing an independent terrestrial ranging source that can continue operating during jamming or spoofing events. R-Mode is being standardised under the auspices of IALA as part of a broader global maritime resilient PNT framework, and is expected to operate synergistically with eLoran, VDES, and other terrestrial systems within a layered approach to maritime navigation resilience.

5.2.3 Pseudolites and Purpose-Built Ranging Networks

Pseudolites and terrestrial ranging networks are a class of ground-based PNT systems in which fixed transmitters radiate GNSS-like signals to enable positioning and/or time transfer using terrestrial infrastructure. Unlike wide-area broadcast systems such as eLoran or R-Mode, and unlike broadcast or mass-market terrestrial positioning systems that derive PNT opportunistically from communications infrastructure, these networks are typically engineered and managed installations, with transmitter geometry, synchronisation, and coverage tailored to a defined operational area.

In most implementations, pseudolite-based systems are deployed to support local or site-specific applications, such as ports, transport hubs, industrial facilities, or other environments where GNSS performance may be unreliable. Multiple transmitters are installed at surveyed locations, and user receivers estimate position using time-of-arrival, phase, or carrier-based observables, applying trilateration or carrier-phase techniques analogous to satellite navigation. When carefully designed and calibrated, such networks can deliver high positioning accuracy, including centimetre-level positioning and sub-nanosecond timing performance in favourable conditions [80].

One of the most well-known commercial implementations of this approach is Locata, which provides a proprietary terrestrial ranging system based on synchronised ground transmitters called LocataLites operating as a managed network. Locata deployments have historically focused on GNSS-challenged environments requiring high reliability and precision, and the system is frequently cited as an exemplar of the broader pseudolite concept rather than a distinct technology category [81].

While local area deployments are the most common use case, terrestrial ranging networks are not inherently limited to small footprints. With sufficient transmitter density, robust inter-transmitter synchronisation, and appropriate operational oversight, such networks can be configured to support regional-scale services, particularly for time distribution. Conceptual architectures described in the literature illustrate how dense terrestrial transmitter networks could be used as wide-area timing backbones, including illustrative deployments covering compact national geographies such as the United Kingdom, where geographic scale and infrastructure density make such an approach theoretically feasible [82]. In these configurations, timing resilience rather than continuous nationwide positioning is the primary objective.

A defining technical challenge for pseudolite and terrestrial ranging networks is time synchronisation across transmitters. Unlike GNSS constellations, which rely on stable onboard atomic clocks, terrestrial systems must maintain precise inter-transmitter timing using local oscillators, wired or wireless distribution links, and continuous monitoring and calibration. Additional challenges include near-far effects, multipath in complex environments, spectrum access and licensing, and receiver interoperability. As a result, these systems tend to be infrastructure-intensive and purpose-built, with achievable performance closely tied to deployment density and operational maturity.

Within a resilient PNT architecture, pseudolites and terrestrial ranging networks are therefore best viewed as complementary infrastructure layers. They are well suited to providing high-confidence positioning in critical locations and, where deployment density allows, resilient timing distribution across regional or compact national footprints. Rather than competing directly with wide-area broadcast or space-based systems, they contribute to a layered approach in which different terrestrial technologies address different spatial scales and resilience requirements.

5.2.4 Broadcast and Mass-Market Terrestrial Positioning and Timing

Broadcast and mass-market terrestrial positioning systems represent a distinct class of PNT technologies that leverage existing high-power communications infrastructure, such as television broadcast and cellular networks, to provide positioning and timing capabilities to large numbers of users. Unlike purpose-built terrestrial radionavigation systems such as pseudolites and managed terrestrial ranging networks, these approaches are characterised by their potential reach, scalability, and integration with consumer devices, reflecting the economics and deployment models of mass-market communications networks.

While the systems described in this section are not considered signals of opportunity in the strict sense, they derive PNT capability from existing broadcast or communications infrastructure rather than from dedicated ranging transmitters. In this respect, they are analogous to emerging LEO PNT approaches that embed or fuse navigation functionality within broader satellite communications systems, whereas pseudolite networks are more closely analogous to deploying fully dedicated PNT constellations (see Section 5.1.2).

A key feature of these systems is their reliance on signals of opportunity or lightly modified broadcast waveforms, rather than dedicated navigation transmissions. Positioning is typically achieved using time-based observables derived from multiple terrestrial transmitters with known locations. Because broadcast and cellular networks are designed primarily for coverage and capacity rather than navigation geometry, achievable positioning performance is highly dependent on transmitter density, network synchronisation, and receiver capability, and varies significantly between urban, suburban, and rural environments.

5.2.4.1 Broadcast Positioning System (BPS)

One prominent example of this class is terrestrial broadcast positioning based on digital television infrastructure, most notably the Broadcast Positioning System (BPS) developed around the next generation ATSC 3.0 standard for television in the United States. BPS exploits precise timing and synchronisation across television transmitters to support ranging and timing at the receiver, and has been demonstrated as a potential source of resilient timing and coarse positioning using widely deployed broadcast infrastructure. Its primary value proposition lies in timing distribution and urban positioning resilience, rather than high-accuracy navigation [83].

5.2.4.2 Dedicated Cellular-Based Positioning Systems

A related but distinct approach is terrestrial cellular positioning using 4G/5G networks, including proprietary and standards-based solutions that exploit dense base-station deployments in metropolitan areas. While the systems described in this section are not considered signals of opportunity in the strict sense, they derive PNT capability from existing broadcast or communications infrastructure rather than from dedicated GNSS-like ranging networks such as pseudolites.

Companies such as NextNav have demonstrated wide-area terrestrial positioning capabilities using dedicated spectrum and purpose-built network configurations [84]. While such systems can provide useful positioning performance in urban environments, they rely on infrastructure investment, spectrum access, and close integration with mobile network operators, and are therefore highly sensitive to national regulatory and commercial contexts.

5.2.4.3 3GPP-Based Mobile Network Positioning

A closely related subset of mass-market terrestrial positioning is based on 5G and emerging 6G mobile networks. Positioning capabilities are defined within the 3GPP standards and include methods such as Observed Time Difference of Arrival (OTDOA), Angle of Arrival (AOA), Round-Trip Time (RTT), and multi-cell TDOA, enabling position determination that does not rely solely on GNSS. From 3GPP Release 16 onwards, additional support for

positioning correction services and enhanced network calibration has been introduced, improving achievable performance in dense deployments. While such capabilities can deliver sub-metre positioning under favourable urban conditions, they remain highly dependent on network density, synchronisation, and commercial operating models [85].

In addition to positioning, mobile networks distribute precise time to base stations for synchronisation, typically traceable to UTC via GNSS. In 5G and future 6G architectures, timing resilience can be enhanced through network-based time transfer mechanisms, including IEEE 1588 Precision Time Protocol (PTP) over fibre and microwave backhaul, and the use of local oscillators or atomic clocks at key nodes. In such configurations, mobile networks may maintain useful timing performance during GNSS outages, although this capability is implementation-dependent and not universally available.

5.2.4.4 Use of AM and FM Broadcast Signals for Timing and Navigation

AM and FM broadcast radio signals have been proposed as potential terrestrial PNT references due to their widespread geographic coverage, high effective radiated power, and long-term operational stability of national broadcast infrastructure. In principle, these signals can support timing or coarse positioning through time, phase, or frequency-based observables, particularly where transmitter locations and network synchronisation characteristics are well characterised. AM and FM broadcast services operate in markedly different frequency bands, with AM transmissions typically occupying the medium-frequency (MF) spectrum (approximately 100-1700 kHz) and FM services operating in the very high frequency (VHF) band (approximately 78-108 MHz). These frequency differences result in distinct propagation characteristics, coverage patterns, and interference behaviours, which in turn influence their suitability for timing or navigation applications.

Unlike purpose-built radionavigation systems, AM and FM broadcasts were not designed with navigation integrity or assurance requirements in mind, however, their ubiquity and propagation characteristics make them candidates for further investigation as complementary PNT inputs. The extent to which such signals could contribute meaningfully to resilient PNT depends on achievable accuracy, stability, interference susceptibility, network synchronisation practices, and the ability to characterise and monitor performance under operational conditions. As such, their role, if any, would need to be established through systematic testing, validation, and governance assessment rather than assumed a priori.

5.2.4.5 Resilience Implications and Architectural Considerations

From a resilience perspective, broadcast and mass-market terrestrial positioning systems offer both opportunities and limitations. Their strengths lie in infrastructure ubiquity, high transmitted power, and the potential to reach large user populations using existing devices. However, they typically depend on complex network synchronisation, commercial operating models, and infrastructure that is not designed or governed primarily as safety-of-life navigation systems. As a result, their suitability as components of a national resilient PNT architecture depends on factors such as governance, service guarantees, interoperability, and alignment with critical-infrastructure requirements.

Within the context of this report, broadcast and mass-market terrestrial positioning systems are best viewed as adjunct layers within a broader system-of-systems approach. They may provide valuable resilience benefits for specific use cases, particularly urban positioning and timing continuity, but are unlikely to substitute for dedicated terrestrial radionavigation systems or satellite-based services on a standalone basis.

5.3 Time transfer, synchronisation and holdover

Precise time is a foundational element of any modern PNT infrastructure. Beyond navigation, accurate time underpins telecommunications, energy distribution, finance, broadcast media, and defence operations. Many of these systems require synchronisation to sub-microsecond levels, and even brief loss of timing accuracy can result in degraded performance, service outages, or safety risks. Unlike positioning failures, timing degradation can propagate silently across interconnected systems, making it a high-impact, but often low-visibility risk for critical infrastructure. While satellite-based timing services are a primary delivery method, robust PNT architectures require resilient time transfer mechanisms, precise synchronisation, and adequate holdover capability to ensure continuity during disruption or degradation.

5.3.1 Time Transfer

Time transfer is the process of delivering a precise and traceable time scale (often UTC or a closely aligned derivative) from a trusted reference source to a remote user or system. The goal is not only to provide the correct time-of-day, but to ensure that the delivered time maintains the required accuracy, stability, and traceability to an internationally recognised standard. This process is essential for any application where coordinated operation or accurate timestamping is critical, such as telecommunications, broadcasting, power grid synchronisation, financial transactions, and defence operations in contested environments. Multiple methods exist for time transfer, each with different performance characteristics, infrastructure requirements, and resilience profiles.

Unlike time-of-arrival (TOA) or time-difference-of-arrival (TDOA) ranging techniques used for positioning, time transfer assumes that the signal path and relative geometry between transmitter and receiver are known or calibrated, such that the primary objective is clock synchronisation rather than distance estimation. This is delivered through a narrower band and directional, two-way link, where only the clock components of the two receivers and transmitters are calculated.

In GNSS, this distinction is reflected in the separation between user positioning, where receiver clock bias is estimated as part of a one-way ranging solution, and system time maintenance, where satellite clocks are synchronised to a reference timescale using dedicated control-segment time transfer links rather than user-level ranging observations.

5.3.1.1 Satellite Time Transfer

Satellite-based time transfer is most commonly achieved through one-way reception of GNSS signals, such as GPS and Galileo, which provide traceable access to UTC at global scale. GNSS timing offers high accuracy, wide availability, and low receiver complexity, making it the dominant timing source across many civil, commercial, and defence applications.

In addition to GNSS, other satellite-based timing approaches are used to improve resilience and reduce dependence on a single signal type or orbital regime. Two-way techniques, such as Two-Way Satellite Time and Frequency Transfer (TWSTFT), enable precise time comparison between sites by compensating for propagation delays and are widely used in metrology and defence contexts [86]. TWSTFT is delivered by GEO spacecraft, which are lower latency than MEO, and also by their two-way nature, have lower throughput. The systems are expensive to build, launch and operation.

Beyond radio-frequency techniques, optical time transfer is emerging as a promising pathway for next-generation satellite timing. The European Space Agency's Optical Synchronised Time and Ranging (OpSTAR) mission is an in-orbit demonstrator designed to validate laser-based two-way time transfer and inter-satellite ranging for future PNT architectures. OpSTAR targets picosecond-level clock synchronisation between satellites and between space and ground, significantly exceeding the performance of current GNSS-based timing. By exploiting optical inter-satellite and ground-to-space links, the mission explores highly resilient and autonomous timing concepts, including distributed clock ensembles and reduced dependence on continuous ground contact, with the explicit aim of de-risking optical technologies for future GNSS and multi-layer PNT systems [87].

Commercial satellite timing services have also emerged (Table 24), providing managed time delivery independent of conventional GNSS signals. Examples include Fugro AtomiChron®, which delivers timing from geostationary orbit, and Iridium STL, which provides timing services from low Earth orbit. Table 24 provides high-level architectural comparison of satellite-based timing delivery mechanisms. GNSS is included as a reference baseline to illustrate differences in orbital regime, signal delivery, and assurance characteristics. The table does not compare performance or accuracy of the different services.

From a resilience perspective, the key distinction between these approaches lies not in raw timing accuracy, but in their architectural diversity and independence from common-mode GNSS failure mechanisms.

Table 24: Satellite-based Timing Services.

System	Orbit Regime	Signal Delivery	Frequency Allocation	Authentication / Integrity Features	Operation Mode
GNSS (baseline)	MEO	One-way Broadcast	GNSS L-band	Limited (constellation and signal dependent)	Fully operational, public service
Fugro AtomiChron®	GEO	One-way Broadcast	Non-GNSS L-band (GEO broadcast)	Signal authentication and service assurance	Fully operational, commercial service
Iridium STL	LEO	One-way Broadcast	Non-GNSS L-band	Signal authentication and service assurance	Fully operational, commercial service

These non-GNSS satellite timing services typically employ alternative signal structures, frequency bands, and orbital geometries, helping to reduce susceptibility to common-mode failures affecting GNSS. By diversifying both the physical layer and space segment, they can provide valuable redundancy in environments where GNSS availability or integrity is degraded.

Looking ahead, dedicated LEO PNT constellations and 5G non-terrestrial network (NTN) architectures are also being explored for their potential to deliver resilient satellite-based timing, particularly in contested or interference-prone environments (see Section 5.1.2).

5.3.1.2 Terrestrial Time Transfer

Terrestrial time transfer methods range from dedicated physical links, such as fibre-optic connections capable of delivering sub-nanosecond accuracy over hundreds of kilometres, to packet-based protocols such as Network Time Protocol (NTP) and Precision Time Protocol (PTP) operating over standard IP networks. Some terrestrial broadcast PNT systems also incorporate network-level time transfer mechanisms to discipline and synchronise distributed transmitter sites, complementing user-facing time distribution methods.

In specialist environments, enhanced protocols such as White Rabbit, combine PTP with synchronous ethernet and phase measurements to achieve sub-nanosecond synchronisation across distributed systems [85]. Another widely used method is Inter-Range Instrumentation Group time code (IRIG-B), a standardised time code distributed over electrical or optical signals, which provides millisecond-level synchronisation and remains common in power grids, test ranges, and legacy timing systems [89].

The choice of method depends on the accuracy and stability required, the availability of infrastructure, and the resilience needs of the application. For instance, national metrology institutes often rely on specialised techniques such as TWSTFT and fibre-optic links for inter-laboratory comparisons at the nanosecond level, while most corporate IT systems depend on NTP for millisecond-level accuracy. As PNT resilience becomes a greater priority, organisations are increasingly adopting hybrid approaches combining satellite, terrestrial, and network-based time transfer to mitigate single points of failure and to ensure continuity in contested or degraded environments.

Additionally, there are technologies that can improve the performance of one of the standard protocols. One example includes the Robust Absolute and Difference Clock (RADClock) approach, which can improve the performance of standard NTP time transfer by timestamping packets against a raw hardware counter and applying minimum-delay filtering [90]. RADClock can maintain the stability of both an absolute clock and a difference clock in parallel, allowing the difference clock to remain stable even during long network outages, providing sub-microsecond accuracy over days without external references.

Table 25 presents the various timing protocols along with their typical accuracies, key features and primary use cases.

Table 25: Timing protocols including key features and primary use cases.

Protocol	Typical Accuracy	Key Features	Primary Use Cases
NTP	Few ms over WAN 1-50 ms on LAN	Oldest & most widely used protocol, hierarchical (stratum-based) architecture, works over IP networks.	General-purpose time sync for computers, servers, IT systems, logging, monitoring.
PTP (IEEE 1588)	Sub-microsecond (µs), typically <1 µs on LAN	Hardware timestamping, boundary and transparent clocks, high precision over Ethernet.	Telecom networks, industrial automation, financial trading, power systems, Broadcast.
White Rabbit	<1 ns (sub-nanosecond)	Extension of PTP + SyncE, measures fibre delay asymmetry, deterministic accuracy.	Financial Trading, telecom backbone timing, critical infrastructures, scientific experiments, time-keeping laboratories.
GNSS-based Sync	10-100 ns (depending on receiver type)	Uses satellite signals for absolute time reference, performance depends on antenna environment.	Telecom base stations, mobile networks (4G/5G), power grids (Substation Sync), outdoor distributed systems
IRIG-B	1-10 µs	Encoded time signals over dedicated lines (analog/digital), very robust.	Military, aerospace, test ranges, Power utilities, legacy systems.

Typical accuracies in Table 25 are indicative and depend on various factors, such as network conditions, hardware support, and deployment architecture.

5.3.2 Time Synchronisation

Time synchronisation is the process of ensuring that multiple clocks or systems remain aligned to a common time scale, both in rate and in epoch. In practice, this requires systems to operate at the same frequency, maintain consistent phase relationships, and align absolute time, typically to UTC or a closely related timescale. Accurate synchronisation underpins coordinated operation across distributed systems, enabling coherent scheduling, event ordering, and time-stamping in both civil and defence applications.

Unlike time transfer, which focuses on delivering a reference time to a location, time synchronisation concerns how that reference is applied and maintained across a network of devices. Synchronisation performance is therefore influenced not only by the quality of the external time source, but also by internal clock stability, network asymmetries, latency variation, and the design of the synchronisation architecture itself. As systems become more distributed and interconnected, maintaining tight synchronisation becomes increasingly challenging, particularly under degraded or contested conditions.

There are three principal aspects of time synchronisation:

- Frequency synchronisation, which ensures that clocks run at the same rate and do not drift relative to one another over time.
- Phase synchronisation, which aligns timing epochs so that events occur simultaneously across systems.
- Time-of-day synchronisation, which aligns clocks to a common absolute time reference to support coherent time-stamping and scheduling [91].

Different applications place different emphasis on these aspects. For example, telecommunications networks prioritise frequency and phase synchronisation to support carrier alignment and handover, while financial systems and distributed sensing applications require accurate time-of-day synchronisation to ensure consistent transaction ordering and data fusion.

From a resilience perspective, synchronisation architectures represent a critical vulnerability. Many systems rely on a single external reference, most commonly GNSS, to discipline large numbers of downstream clocks. When this reference is disrupted, synchronisation errors can propagate rapidly through networks, leading to cascading failures even if local clocks remain operational [92]. In some cases, systems may continue operating with internally consistent, but globally incorrect time, making faults difficult to detect and diagnose.

To address these risks, resilient synchronisation architectures increasingly adopt a multi-layered approach. This typically combines multiple independent time inputs, such as GNSS, terrestrial broadcast timing, and secure fibre-based references, with local high-stability oscillators capable of maintaining synchronisation during outages. Continuous monitoring and cross-checking of time sources are used to detect divergence, while automated selection and fallback mechanisms enable systems to degrade gracefully rather than fail abruptly, consistent with documented user requirements for resilient time synchronisation [93].

In defence and other high-assurance environments, synchronisation architectures are further designed to operate in contested conditions. These systems may include authenticated time sources, protected distribution networks, and autonomous modes that prioritise internal coherence when external references are unavailable. Rather than seeking to maintain absolute UTC alignment at all times, such architectures aim to preserve mission-critical synchronisation within defined tolerances until reliable external timing can be restored [94].

The effectiveness of any synchronisation strategy ultimately depends on the interaction between external time transfer, internal clock performance, and the system's ability to detect, manage, and recover from timing degradation. This makes synchronisation a key bridge between time transfer and holdover, and a central consideration in the design of resilient PNT architectures.

5.3.3 Time Holdover

Timing holdover is the capability of a local oscillator to maintain accurate time when its primary external reference, such as GNSS, fibre-based timing, or terrestrial broadcast, is unavailable or degraded. During holdover, the oscillator relies entirely on its intrinsic frequency stability, with timing accuracy degrading predictably over time once external synchronisation is lost.

The required holdover performance varies significantly by application. General IT systems may tolerate timing errors of several milliseconds, while telecommunications networks typically require microsecond-level accuracy to maintain network synchronisation [91, 92]. High-assurance scientific, defence, and critical infrastructure systems often demand nanosecond-level stability for extended periods, particularly where timing errors can propagate through networks and cause cascading system failures [93, 94].

In practice, holdover is not a binary capability, but a time-bounded resilience margin. The duration for which a system can remain within acceptable timing limits depends on oscillator type and quality, the accuracy of pre-outage synchronisation, sensitivity to temperature and ageing effects, and the effectiveness of environmental control. Poor disciplining prior to an outage can significantly reduce usable holdover time, even when high-quality oscillators are employed.

Since no oscillator is perfectly stable over indefinite periods, holdover is best implemented as part of a layered timing architecture rather than a standalone solution. High-stability clocks extend operational continuity during outages, but systems should automatically revert to external timing references as soon as reliable signals are restored. In defence and critical infrastructure contexts, combining multiple independent time sources with robust holdover capability provides the greatest assurance of continuity in contested or degraded environments [95].

Holdover technologies can be broadly divided into classical oscillators and atomic clocks. Classical oscillators, such as Temperature-Compensated Crystal Oscillators (TCXO) and Oven-Controlled Crystal Oscillators (OCXO), offer low cost and power consumption, but limited long-term stability. Atomic clocks, including Chip-Scale Atomic Clocks (CSAC), rubidium, caesium, and hydrogen masers, exploit atomic transitions to deliver significantly improved stability at the cost of increased size, power, and expense [96]. These technologies underpin modern resilient timing architectures, particularly where GNSS denial or degradation is a credible risk.

Beyond oscillator selection, effective holdover implementation also requires continuous monitoring and integrity management. Systems must detect when external references are lost or corrupted, transition cleanly into holdover mode, and provide alarms when timing uncertainty exceeds predefined thresholds. Equally important is controlled re-disciplining following outage recovery, as abrupt corrections can introduce phase discontinuities and secondary failures.

Table 26 summarises the characteristics of common oscillator technologies and their typical holdover performance, defined as the duration for which timing error remains within one microsecond (±1 µs), highlighting the trade-offs between stability, cost, size, and operational use cases.

Table 26: Characteristics of oscillators with holdover defined to a ±1 µs timing error.

Oscillator Type	Holdover Duration	Size	Power	Cost	Typical Application
TCXO	Few minutes	Low	Low	Low	Consumer electronics, telecom, IoT devices.
OCXO	3-4 hours	Low	Low	Low	Telecom networks, instrumentation, GNSS holdover.
CSAC	3-4 days	Low	Low	Low	Portable systems, defence, GNSS-denied environments.
Rubidium Atomic Clock	3-4 days	Low/Med	Low/Med	Medium	Telecom, power grids, GNSS backup, scientific instruments.
Passive Hydrogen Maser	1-2 weeks	Medium	Medium	High	National metrology institutes, deep-space networks.
Caesium Beam Standard	In Years	Medium	Medium	High	National time standards, calibration labs, scientific research, space agencies.
Active Hydrogen Maser	In Years	High	High	Extremely High	National metrology institutes, scientific research, space agencies.
Optical Caesium Beam Standard	In Years	Medium	Medium	High	National time standards, calibration labs, scientific research, space agencies.

5.4 Onboard Sensors

This section examines onboard sensing technologies according to the physical phenomena they exploit, including motion, magnetic fields, gravity fields, and environmental context. Within each category, a distinction is made between established (*classical*) implementations and emerging *quantum* approaches. This structure reflects both current operational practice and anticipated technological trajectories, while maintaining a clear distinction between deployed resilience capabilities and longer-term research trends.

Onboard sensors can be broadly divided into relative and absolute (or quasi-absolute) sensing modalities. Relative sensors, such as inertial measurement units (IMUs), measure changes in motion and orientation over time and therefore accumulate error unless periodically corrected. In contrast, absolute or field-referenced sensors, including gravimetric and magnetic sensors, exploit properties of the surrounding physical environment to provide external constraints on position or attitude, albeit with varying levels of spatial resolution, stability, and susceptibility to disturbance.

While Sections 5.1-5.3 focus on external PNT sources including GNSS, augmentation systems, terrestrial broadcast, and hybrid architectures, resilient PNT cannot be achieved through external signals alone. A critical layer of resilience is provided by onboard sensors, which enable systems to continue operating when external PNT services are degraded, denied, or untrustworthy.

Onboard sensors differ fundamentally from external PNT sources. They do not depend on external radionavigation signals or timing infrastructure, although many exploit environmental fields or physical phenomena that are external to the platform and may be subject to natural variability or deliberate manipulation. Instead, they provide self-contained measurements of motion, orientation, and environmental state. As such, they play a vital role in bridging short-term PNT outages, supporting integrity monitoring and anomaly detection, and enabling graceful degradation in place of abrupt loss of capability.

From a system-of-systems perspective, onboard sensors should not be viewed as standalone alternatives to GNSS, but as complementary elements within a layered resilience architecture. Their value lies in their ability to provide continuity during interference or outages, cross-check external PNT inputs, and support decision-making when confidence in external signals is reduced.

In operational terms, onboard sensors are often the first line of defence against PNT disruption, buying time for systems to adapt, switch modes, or fall back to other sources. This category encompasses a range of sensing technologies that exploit different physical phenomena, each contributing differently to resilience. These comprise inertial sensors that provide self-contained motion estimation, magnetic and gravity-based navigation techniques that anchor positioning to stable geophysical reference fields, and environmental and context-based sensors including Light Detection and Ranging (LiDAR), radar, vision systems, odometry, and celestial systems. Together, these onboard capabilities form a critical internal resilience layer, whose effectiveness depends not on any single sensor, but on how they are combined, interpreted, and governed within the wider PNT architecture.

5.4.1 Inertial Navigation Systems

Inertial navigation or dead reckoning refers to the process of estimating position based on previously determined coordinates, using velocity, heading, and time data. Unlike GNSS, which provides absolute positioning, dead reckoning systems compute relative motion and are essential for navigation when external signals are unavailable or compromised.

5.4.1.1 Classical Inertial Navigation Systems

Classical Inertial Navigation Systems (INS) use accelerometers and gyroscopes to measure linear acceleration and angular velocity. Several sensor technologies exist, including Micro-Electro-Mechanical Systems (MEMS), Dynamically Tuned Gyroscope (DTG), Fibre-Optic Gyroscope (FOG), and Ring Laser Gyroscope (RLG), each exhibiting different performance characteristics and levels of maturity [97]. A summary of the typical performance and trade-offs between these classical inertial sensors is given in Table 27.

Table 27: Characteristics of classical inertial sensors [97].

Type	Principle of operation	Applications	Advantages / Disadvantages
MEMS	Vibrating micro-structures deflect under rotation, sensing angular rate via the Coriolis effect.	Consumer, automotive, UAV/tactical	+ Tiny SWaP, low power/cost – Higher drift, temp sensitivity
DTG	A mechanically suspended spinning mass measures rotation through torque-induced precession.	Aerospace (legacy), missiles, some INS	+ Proven, robust – Bulky, moving parts, largely superseded
FOG	Counter-propagating light in a fibre coil experiences a rotation-induced phase shift (Sagnac effect).	Aviation/marine INS, land vehicles	+ High accuracy, no moving parts – Larger SWaP-C than MEMS
HRG	A vibrating hemispherical resonator detects rotation through distortion of its standing wave pattern.	Space, strategic/nav-grade INS, marine compass	+ Very low noise, high reliability/ radiation hardened – Specialised manufacturing (cost)
RLG	A vibrating hemispherical resonator detects rotation through distortion of its standing wave pattern.	Commercial/military aircraft, ships, spacecraft	+ High accuracy, mature – Lock-in (needs dithering), cost/size

While classical inertial navigation systems are widely deployed and form the backbone of many resilient PNT architectures, their performance ultimately remains constrained by sensor noise and error growth over time, motivating continued research into quantum-based inertial sensing approaches.

5.4.1.2 Quantum Inertial Navigation Systems

Quantum inertial sensors exploit the quantum properties of atoms or solid-state systems to achieve higher stability and accuracy than classical sensors. Instead of relying on mechanical or optical paths alone, they measure interference in matter waves, atomic spin precession, or quantum states that are intrinsically tied to physical constants [98, 99]. Several approaches are under development, each with distinct operating principles and maturity levels, which are described below in Table 28 below.

Table 28: Characteristics of quantum inertial sensors [96].

Technology	Principle of operation	Applications	Advantages / disadvantages
Atomic Interferometer	Laser-cooled atoms are split and recombined; interference of matter waves encodes acceleration or rotation.	Strategic navigation, spacecraft, submarines	+ Ultra-high sensitivity, drift tied to physical constants; – Requires vacuum chambers, laser cooling, bulky
Atomic Vapour	Warm alkali vapour is optically interrogated; inertial forces shift atomic resonance frequencies.	Compact INS, vehicles, potential tactical use	+ Smaller, simpler, room-temperature operation; – Lower sensitivity than cold-atom systems
Nuclear Magnetic Resonance	Uses nuclear spin precession in magnetic fields; frequency shifts track rotation/ acceleration.	Submarines, underground navigation, defence	+ No moving parts, insensitive to acceleration; – Needs strong magnetic shielding, early-stage technology
Solid State Quantum	Defects in crystals (e.g. NV centres in diamond) act as quantum spin sensors; measure phase shifts under inertial forces.	Potential chip-scale INS, defence, commercial	+ Chip-scale potential, integrable; – Still experimental, limited sensitivity vs atom interferometers

Together, these quantum approaches promise to extend navigation holdover beyond what classical sensors can achieve, by offering drift characteristics tied to fundamental physical constants and the potential for extremely low long-term error growth. However, it's important to note that they remain at different stages of maturity. Cold-atom interferometers demonstrate the highest performance, but remain bulky and complex, while vapour-cell and solid-state approaches are progressing toward more compact, rugged devices suitable for field deployment.

5.4.2 Magnetic Anomaly-aided Navigation

Magnetic anomaly-aided navigation (MagNav) exploits spatial variations in the Earth's magnetic field to support navigation, particularly when GNSS signals are unavailable. MagNav compares onboard magnetometer measurements with pre-existing geomagnetic models or magnetic anomaly maps to estimate position. As a passive technique that does not rely on external transmissions, it is inherently resilient to jamming and spoofing. However, performance is strongly influenced by local magnetic disturbances, environmental variability, and sensor limitations. Like inertial systems, magnetometers can be broadly divided into classical and quantum types.

5.4.2.1 Classical MagNav Techniques

Classical MagNav systems are based on established magnetometer technologies that directly measure the Earth's magnetic field. Fluxgate magnetometers are the most widely used, employing a ferromagnetic core driven into saturation by an alternating current. They have long been standard in geophysics, defence, and space applications, offering robust and stable performance. However, their size and sensitivity to platform-induced noise limit their suitability as standalone navigation sensors in dynamic environments.

Magneto-inductive and magneto-resistive sensors represent a more compact alternative, exploiting changes in inductance or electrical resistance under an applied magnetic field. These sensors offer lower size, weight, and power requirements and are well suited to constrained platforms such as UAVs and small satellites [100]. However, they generally provide lower accuracy and stability than fluxgate systems, restricting their use as primary navigation sensors. Table 29 summarises the characteristics of classical MagNav techniques.

Table 29: Characteristics of classical MagNav techniques [96].

Technology	Principle of operation	Applications	Advantages / disadvantages
Fluxgate	Ferromagnetic core driven into saturation by alternating current	Geophysics, defence, spacecraft, baseline MagNav research	+ Proven, robust, stable; – Bulky, sensitive to platform noise
Magneto-inductive; Magneto-resistive	Changes in inductance or resistance under applied magnetic field	UAVs, satellites, compact navigation systems	+ Small, low power, easy integration; – Lower accuracy and stability than fluxgate

Beyond traditional magnetometer-based MagNav approaches, a number of commercial solutions are emerging that combine geomagnetic information with advanced data-driven techniques. AstraNav employs a navigation approach that operates with and without pre-existing geomagnetic maps. The Company's M-GPS® software technology leverages spatial variations and multiple components of the ambient magnetic field, using machine learning to convert local magnetic signatures into high-accuracy navigational data as well as generating high resolution geomagnetic maps as a global positioning reference. This approach enables positioning in GNSS-denied environments using mass-market magnetometer sensors, including those integrated in mobile devices [101].

Similarly, iDvera focuses on trust and integrity layers for alternative PNT sources. Its Anchored Location Integrity System (ALIS) operates as an assurance layer rather than a standalone navigation solution, treating position as a claim to be validated. ALIS integrates alternative signals, such as magnetic navigation, within a governed framework that assesses data consistency, confidence, and resilience across multiple sensing modalities [102].

Together, these patented approaches illustrate how MagNav concepts are increasingly being realised through software-centric architectures that fuse environmental signals with AI-based inference rather than relying solely on specialised hardware.

5.4.2.2 Quantum MagNav Techniques

Quantum magnetometers exploit atomic and solid-state quantum effects to achieve sensitivities beyond those of classical devices, significantly expanding the potential role of magnetic anomaly-aided navigation in GNSS-challenged environments. Optically pumped magnetometers (OPMs) represent the most mature quantum MagNav technology, using alkali vapour cells and laser interrogation to measure magnetic fields with high sensitivity at room temperature. Recent trials have demonstrated that compact OPM-based systems, when combined with advanced denoising and map-matching techniques, can provide competitive navigation performance in selected flight and ground scenarios [103].

Superconducting quantum interference devices (SQUIDs) offer exceptional magnetic sensitivity and underpin high-resolution anomaly mapping efforts. However, their reliance on cryogenic cooling continues to limit their suitability for mobile or size-constrained platforms. Solid-state nitrogen-vacancy (NV) diamond sensors provide an alternative quantum approach, offering vector magnetic field measurements at room temperature in compact and robust form factors. While still maturing, early demonstrations indicate potential for integration into mobile and airborne platforms [99].

Together, these quantum MagNav approaches illustrate a transition from laboratory-scale instruments toward operationally relevant sensing technologies. Each presents distinct trade-offs in sensitivity, size, environmental robustness, and deployment complexity, reinforcing their role as complementary components within layered PNT architectures rather than standalone navigation solutions. Table 30 summarises the characteristics of quantum MagNav techniques.

Table 30: Characteristics of quantum MagNav techniques [96].

Type	Principle of operation	Applications	Advantages / disadvantages
Optically Pumped Magnetometers	Measure spin precession in alkali vapour cells using laser interrogation	Magnetic anomaly navigation, defence, geophysics, biomagnetism	+ High sensitivity, compact, room-temperature operation; – Sensitive to orientation and environmental noise
Superconducting Quantum Interference Devices	Detect quantised magnetic flux in superconducting loops (Josephson junctions)	Anomaly mapping, mineral exploration, biomagnetism	+ Benchmark sensitivity and stability; – Requires cryogenics, bulky for mobile platforms
Nitrogen-Vacancy Centres in Diamond	Use quantum spin states of diamond lattice defects, optically read out	Vector magnetometry, UAVs, mobile platforms, defence	+ Room-temperature operation, vector capability, robust; – Lower sensitivity than lab-based OPM/SQUID, still maturing

Taken together, magnetic anomaly-aided navigation illustrates the potential of exploiting stable geophysical reference fields to support positioning in GNSS-challenged environments. Both classical and quantum MagNav techniques offer valuable resilience benefits as passive, non-emitting sensors, but their effectiveness remains strongly dependent on environmental conditions, map quality, and platform integration. As such, MagNav is best understood as a complementary capability within layered PNT architectures, rather than a standalone navigation solution.

5.4.3 Gravitational Anomaly-aided Navigation

Gravitational anomaly-aided navigation (GravNav) exploits spatial variations in the Earth's gravitational field as a reference for navigation. By measuring local gravity or gravity gradients and comparing them with pre-existing anomaly maps, platforms can estimate position independently of GNSS. GravNav is inherently passive and resistant to RF interference, but its performance depends critically on the resolution and accuracy of available gravity maps. In practice, GravNav is generally limited to horizontal (2D) positioning, with degraded performance in regions of low gravity contrast or dead zones. While MagNav is often better suited to airborne environments, GravNav shows greater potential in maritime and subsea applications [98].

5.4.3.1 Classical GravNav Techniques

Early GravNav instruments were mechanical or optical accelerometer-based gravimeters that measured the deflection of a suspended mass under gravity. While foundational to geophysical surveying, these systems were bulky, slow, and required highly controlled environments.

More recent developments include MEMS gravimeters, which miniaturise gravimetric sensing into compact, low-power devices suitable for mobile platforms such as submarines and autonomous vehicles. However, challenges remain in thermal stability, calibration, and long-term drift.

Falling corner cube gravimeters represent another classical approach, tracking a retroreflector in free fall using laser interferometry. These systems offer high sensitivity but are large and vibration-sensitive, restricting their use primarily to laboratory and survey applications rather than real-time navigation. Table 31 summarises the characteristics of classical GravNav techniques.

Table 31: Characteristics of quantum MagNav techniques [96].

Type	Principle of operation	Applications	Advantages / disadvantages
Mechanical / Optical	Deflection of a suspended mass under gravity	Submarine navigation, geophysics surveys	+ Robust, proven; – Bulky, requires controlled environment
MEMS	Micrometre-scale accelerometers measuring gravity	Autonomous vehicles, mobile platforms	+ Small, low power; – Thermal drift, calibration and stability challenges
Falling Corner Cube	Retroreflector in free fall tracked by laser interferometry	Surveying, laboratory, gravity mapping	+ High sensitivity; – Vibration-sensitive, not suited to real-time or mobile applications

5.4.3.2 Quantum GravNav Techniques

Quantum gravimeters represent a significant advance over classical gravimetric sensors by exploiting atomic interferometry to measure gravity with exceptional sensitivity and long-term stability. By tracking the free-fall trajectories of laser-cooled atoms, these instruments detect minute variations in gravitational acceleration through matter-wave interference. Compared with mechanical or MEMS gravimeters, quantum systems exhibit reduced long-term drift, enabling extended autonomous operation with less frequent recalibration.

Atomic interferometer gravimeters determine local gravitational acceleration by monitoring changes in the motion of freely falling atoms, allowing subtle spatial variations in gravity to be resolved [98].

Closely related atomic gravity gradiometers extend this concept by comparing the acceleration of multiple atom clouds, improving sensitivity in regions with weak gravity contrast and enhancing map-matching performance.

Superconducting gravimeters based on SQUID technology also offer benchmark sensitivity, but their reliance on cryogenic cooling and substantial supporting infrastructure confines their use primarily to laboratory and survey applications. While cold-atom gravimetry remains at an early stage of operational maturity, ongoing advances in size, robustness, and integration suggest a gradual transition from experimental demonstrations toward deployable systems in selected defence and geophysical applications. Table 32 summarises the characteristics of quantum GravNav techniques.

Table 32: Characteristics of quantum GravNav techniques [96].

Type	Principle of operation	Applications	Advantages / disadvantages
Atomic Interferometers	Matter-wave interference of cold atoms measures gravitational acceleration.	Submarines, naval platforms, underground navigation	+ High sensitivity, reduced drift, long-term stability; – Bulky, complex, early stage
Atomic Gravity Gradiometers	Differential acceleration of multiple atom clouds in free fall measures gravity gradients.	Map-matching, navigation in low-gradient areas	+ Improved map fidelity, higher accuracy; – Technically challenging, still experimental
Superconducting Devices	Detect quantised magnetic flux changes induced by gravity-driven mass motion.	High-sensitivity gravity mapping, research	+ Benchmark sensitivity; – Requires cryogenics, impractical for mobile platforms

Together, quantum GravNav techniques highlight the potential of gravity-based sensing to provide highly stable navigation references in GNSS-challenged environments. While current implementations remain constrained by size, complexity, and deployment conditions, their sensitivity and low drift make them attractive for niche applications where long-term stability is prioritised over real-time responsiveness. As with magnetic and inertial approaches, quantum GravNav is best viewed as a complementary capability within layered PNT architectures.

5.4.4 Environmental and Context-based Onboard Sensors

Unlike inertial, magnetic, or gravitational techniques, environmental and context-based sensors derive navigation information from interaction with the surrounding physical environment. Their effectiveness therefore depends on the presence of distinctive features, structures, or surfaces that can be reliably observed over time. In environments where such features are available, these sensors can provide highly informative relative positioning and situational awareness even in the absence of external PNT signals.

From a resilience perspective, the primary value of these sensors lies in their ability to constrain drift, validate motion estimates, and support localisation during periods of GNSS disruption. When integrated with inertial systems and geophysical reference methods, they contribute to robust multi-sensor fusion architectures that can adapt dynamically to environmental conditions.

However, their dependence on environmental observability, computational resources, and prior mapping underscores the importance of careful system design and performance assurance, particularly for safety-critical applications. Characteristics of these systems are summarised in Table 33 below.

Table 33: Characteristics of environmental and context-based onboard sensors.

Type	Principle of operation	Applications	Advantages / disadvantages
LiDAR	Emits laser pulses and measures return time to build 3D point clouds	Autonomous vehicles, UAV mapping, obstacle avoidance	+ High-resolution 3D models, accurate ranging – Weather/visibility limitations, power-hungry
Radar	Transmits radio waves and analyses reflections to detect objects and surfaces	Aviation, maritime navigation, terrain referencing	+ All-weather, long range, robust – Lower spatial resolution compared to LiDAR/vision
Vision	Cameras with image processing algorithms for feature recognition	Drones, robotics, handheld navigation aids	+ Lightweight, passive, low-cost – Sensitive to lighting, cluttered or changing environments
Celestial	Uses observations of celestial bodies to estimate position and attitude.	Maritime navigation, space navigation.	+ GNSS-independent, passive - Requires clear sky conditions and accurate time reference

Together, these technologies provide complementary capabilities that, when integrated with classical and quantum navigation methods, enable multi-sensor fusion frameworks designed to sustain resilient, all-weather navigation under disruption.

5.5 User Equipment Hardening and Resilience

User equipment is often the first line of defence against disruption or manipulation of GNSS signals. While system-level measures and complementary PNT sources are important, a substantial proportion of practical resilience is achieved at the level of the receiver and its directly associated hardware. Advances in antenna technology, receiver design, and embedded sensing allow modern GNSS equipment to better detect, resist, and recover from interference and spoofing.

In addition to physical and RF hardening, resilient user equipment increasingly incorporates monitoring, detection, and adaptive behaviours that allow systems to maintain trusted operation under degraded conditions. These capabilities are realised in practice through a combination of advanced antenna technologies and increasingly intelligent receiver architectures, which together form the core of user-level PNT hardening. In this context, hardening refers to physical and RF-level protection, while resilience encompasses detection, adaptation, and recovery behaviours under degraded conditions.

5.5.1 Controlled Reception Pattern Antennas

Controlled Reception Pattern Antennas (CRPAs) strengthen resilience by using multiple antenna elements, typically arranged in a circular or array configuration, rather than a single element as in conventional GNSS antennas. Each element receives the same satellite signals as well as any interference or spoofing signals arriving from different directions. By comparing the phase and amplitude across the elements, the receiver can estimate the direction of arrival of each signal [104].

This enables the antenna system to apply adaptive beamforming as follows:

- Signals coming from the direction of genuine satellites (spread across the sky) are reinforced, creating high-gain beams that preserve their integrity.
- Signals identified as interference, such as a jammer on the horizon or a spoofing re-radiator, are actively suppressed by steering spatial nulls toward those directions.
- Because satellites are distributed across the sky, the CRPA can suppress threats from a few azimuths while continuing to track authentic signals from elsewhere, maintaining navigation capability even in contested environments.

In practice, CRPAs allow a receiver to block or ignore signals from hostile sources while continuing to process the remainder of the constellation. This makes them one of the most effective user-equipment countermeasures against both jamming and spoofing. Their drawbacks are that they require additional elements, processing power, and careful calibration, and they may introduce small biases that affect the most demanding precision applications.

CRPAs have historically faced regulatory constraints. Until recently, they were listed under the International Traffic in Arms Regulations (ITAR) as defence-sensitive equipment.

This designation severely limited US manufacturers' ability to export CRPAs, impeding innovation and broad civilian adoption, particularly in aviation, autonomous vehicles, and critical infrastructure applications. That changed in January 2025 when the US Department of State published a rule reclassifying CRPAs for PNT from the US Munitions List (USML) to the less restrictive Export Administration Regulations (EAR) regime, under the Department of Commerce [105].

While CRPAs address interference at the antenna level, their effectiveness is maximised when combined with receiver architectures capable of signal quality assessment, anomaly detection, and adaptive positioning strategies.

5.5.2 Intelligent Receivers

Modern GNSS receivers are no longer simple black boxes that output position and time. These days the receivers incorporate a growing set of resilience-focused features designed to detect, resist, and recover from interference or spoofing. These features are often grouped under the idea of intelligent receivers, where advanced signal processing and cross-checking methods are embedded directly into the user equipment. Key capabilities of intelligent receivers include:

- **Multi-constellation, multi-frequency tracking –** by simultaneously processing signals from GPS, Galileo, BeiDou, GLONASS, and others across several frequency bands, receivers reduce the risk that all signals can be disrupted at once. A spoofer or jammer must target many more signals, raising the technical barrier for an attacker.
- **LEO PNT capabilities –** receiver manufacturers are already starting to incorporate signals from upcoming LEO PNT constellations into their receivers, which will become available in a few years' time, thus extending resilience by providing an entirely separate layer of satellite signals that are stronger, more dynamic, and harder to jam and spoof than traditional GNSS.
- **Adaptive tracking architectures –** advanced tracking loops, such as vector tracking, make use of information across satellites rather than treating each signal independently. This allows receivers to maintain lock under weak-signal conditions, during high dynamics, or in the presence of structured interference.
- **Built-in interference monitoring –** receivers can continuously monitor internal metrics such as automatic gain control (AGC), carrier-to-noise ratio (C/N_o), and Doppler residuals. Abnormal behaviour in these parameters often provides the earliest clues of jamming or spoofing, allowing the receiver to flag suspect signals.
- **Fault detection and exclusion –** integrity algorithms such as Receiver Autonomous Integrity Monitoring (RAIM) and Advanced RAIM (ARAIM) use redundancy across satellites to detect and exclude inconsistent signals. This prevents a single manipulated or faulty signal from corrupting the overall solution.
- **Situational awareness and logging –** intelligent receivers not only react in real time, but also log anomalies for later analysis. This supports both operational response and the continuous improvement of resilience strategies.

Together, these features allow intelligent receivers to act as active participants in resilience, rather than passive consumers of GNSS signals. While no single method guarantees protection, their combination greatly improves the ability of user equipment to continue providing trustworthy PNT in contested environments.

Ultimately, user equipment hardening and resilience measures determine how effectively higher-level PNT architectures translate into trusted positioning and timing at the point of use.

5.6 AI/ML as Cross-Cutting Enablers for Resilient PNT

Artificial intelligence (AI) and machine learning (ML) are increasingly being applied across the PNT ecosystem to enhance robustness, adaptability, and situational awareness in complex and contested environments. AI can be treated as an umbrella term for computational methods that support perception, reasoning and decision support, while ML refers more narrowly to data-driven techniques that learn patterns from examples. This distinction is important in resilient PNT because AI is often used loosely, whereas most practical progress has been realised through task-specific ML components embedded within existing navigation, signal processing and integrity-monitoring architectures [106].

In this chapter, AI is considered specifically as an enabling computational layer within PNT systems supporting perception, inference, and decision support at the navigation and integrity level, and intentionally not treated as an autonomous capability, governance domain, or a threat vector in its own right.

5.6.1 Machine learning in resilient PNT architectures

A systematic review of ML applications in GNSS indicates that this is not a niche topic. In total, 213 studies were published between 2000 and 2021, spanning ten categories of ML approaches, and show that ML methods frequently achieve acceptable performance and can outperform traditional techniques in challenging conditions. The key implication for resilience is not that ML replaces deterministic navigation, but that it can improve robustness where classical models are limited by unmodelled effects, non-stationary error behaviour, or incomplete observability [107].

One of the most mature and defensible roles for ML in resilient PNT is in detection and classification tasks, including learning to recognise anomalous patterns in RF observables, correlator outputs, measurements, or solution-level residuals. These methods can help discriminate between nominal degradation (e.g., multipath and signal attenuation), and intentional interference (e.g., jamming, spoofing), particularly where threat signatures evolve and are difficult to capture using fixed thresholds [106].

While public technical detail is often limited, industry reporting indicates an ongoing transition from research to fieldable implementations for edge-deployed threat detection. Vendor-reported solutions describe ML-based GPS threat detection designed for software-defined radios and embedded systems, aiming to rapidly detect and classify low-power threats and support the sharing of threat characterisation across users. ML is also used to improve perception of the RF environment and to inform higher-level response and reconfiguration mechanisms, rather than acting as a standalone navigation engine [108].

Resilient PNT increasingly relies on combining GNSS with inertial sensors, vision, mapping constraints, terrestrial signals, and platform context. Classical estimators (e.g., Kalman filters) remain foundational, while ML is increasingly used to adapt parameters, learn error models, and manage context-dependent sensor weighting within hybrid architectures [109].

Across these use cases, the consistent pattern is that ML is most valuable when it is bounded, explainable at the system level, and integrated into multi-layer architectures, as follows:

- **Perception –** detecting and characterising interference and abnormal behaviours from RF and navigation observables.
- **Adaptation –** context-aware weighting and parameter tuning for multi-sensor estimators (hybrid ML + classical filtering).
- **Engineering leverage –** synthetic data generation, simulation realism, and optimisation to broaden test coverage and accelerate development.
- **Trust outputs** – producing confidence/assurance metrics suitable for operational decision-making, not just coordinates.

5.6.2 AI-derived GNSS-independent positioning

Alongside hybrid GNSS-plus-sensor approaches, a small but growing class of solutions seeks to deliver GNSS-independent positioning by inferring location primarily from onboard sensors, digital maps, and data-driven models. These approaches are often presented as *AI-based* alternatives because they aim to maintain a continuous position estimate when external signals are unavailable, unreliable, or untrusted, using software-only methods that exploit context and learned relationships rather than relying on satellite ranging.

One example is a vehicle focused Independently Derived Positioning System (IDPS) concept developed and trademarked by Tern.AI that combines base maps with vehicle sensor data and a proprietary AI engine to estimate position without satellite signals [110]. Notably, this approach has been selected for evaluation under the US Department of Transportation's Complementary PNT rapid-phase field testing programme for high-TRL solutions, indicating active interest in assessing such methods within operationally oriented test campaigns [111]. As with other AI-first alternatives, published performance characterisation and independent validation remain limited, and operational utility will depend on the outcomes of structured test and evaluation campaigns.

In summary, AI/ML can be treated within the technology landscape as a cross-cutting resilience layer that strengthens detection, fusion, and assurance functions. The available evidence indicates substantial research activity and promising results across GNSS use cases, alongside an emphasis in institutional and programme literature on validation, explainability, and test realism as prerequisites for wider deployment in safety- and mission-critical contexts [107, 109].

5.7 Chapter Summary

This chapter has examined the evolving landscape of resilient PNT through the lens of diversity, layering, and system integration. It has shown that no single technology, whether satellite-based, terrestrial, or onboard, can provide assured PNT under all conditions. Instead, resilience emerges from architectures that combine multiple, complementary sources with different failure modes and threat sensitivities.

External PNT services, including modernised GNSS, augmentation systems, terrestrial broadcasts, and emerging LEO-based capabilities, continue to provide the backbone of positioning and timing for most users. However, their vulnerability to interference, spoofing, and space-weather effects reinforces the need for additional layers of assurance. Terrestrial broadcast systems, operating at different frequencies and with fundamentally different propagation characteristics, can provide complementary positioning and timing information that is inherently more robust to certain classes of interference and space-weather effects. Onboard sensors play a critical role in bridging outages, cross-checking external signals, and enabling graceful degradation rather than abrupt loss of capability.

The chapter has also highlighted the growing importance of user equipment hardening and resilience. Advances in antenna technologies and the emergence of increasingly intelligent receiver architectures are shifting resilience from a purely system-level concern to one that is actively managed at the point of use. These developments enable detection, adaptation, and recovery behaviours that are essential in contested and degraded environments.

Taken together, the technologies reviewed in this chapter underscore a central conclusion, namely that resilient PNT is not achieved through substitution, but through integration. Effective solutions depend on how diverse PNT sources and sensors are combined, governed, and trusted within a coherent system-of-systems framework. This sets the foundation for the next chapter, which considers how these technical capabilities translate into operational practices, governance mechanisms, and policy choices for strengthening national PNT resilience.

6 CONCEPTUAL RESILIENT PNT ARCHITECTURES

The consequences of PNT disruption cut across Defence, civil government, industry, and the public. Chapter 6 therefore proposes how risks posed by PNT threats can be met by a combination of governance and policy measures, paired with technical resilience. Consequently, this chapter builds on this analysis by examining how technology options can be structured to strengthen Australia's national PNT posture.

6.1 PNT Resilience Levers

Comprehensive examinations of the definition of PNT resilience have been covered extensively in the literature [1, 50]. This report does not purport to define or duplicate what resilience entails. This section briefly considers P*NT resilience* beyond technical challenges by examining how combinations of system design, governance arrangements, policy settings, and technological capabilities can help mitigate the PNT hazards or threats.

It is proposed that one or more of four resilience levers – System, Governance, Policy, Technology – can be activated to mitigate each of the PNT-related hazard classes. Table 34 illustrates how integration of the high-level levers, as well as lower-level examples, could contribute to resilience.

Table 34: Hazard-driven PNT resilience levers can be activated together to achieve resilience objectives.

Hazard class	Resilience levers	Resilience objective
Natural (baseline moderate – severe consequence)	**System**	
	• PNT-dependent system hardening and recovery • Distributed architectures	• Limit mission impact by reducing geographic and systemic failure • Enable timely recovery of PNT-dependent functions following environmental disruption
	Governance	
	• National and institutional coordination frameworks	• Ensure coordinated preparedness, response, recovery across PNT-reliant sectors
	Technology	
	• Multi-layered space-based PNT • Terrestrial-based PNT • Enhanced timing holdover	• Assure wide-area PNT availability • Provide continuity of PNT services independent of space systems • Preserve essential timing functions during temporary PNT loss
Physical (escalating consequence in competition and conflict)	**Governance**	
	• National and institutional coordination frameworks	• Ensure coordinated preparedness, response, recovery across PNT-reliant sectors
	Technology	
	• Multi-layered space-based PNT • Terrestrial-based PNT	• Limit operational vulnerability from loss of a single system (i.e. GPS) or provider • Maintain operational continuity under kinetic or infrastructure damage
Cyber, information and EM (persistent across competition spectrum)	**Governance**	
	• National and institutional coordination frameworks	• Enabled coordinated detection, attribution, and response to persistent cyber and RF interference
	Technology	
	• Multi-layered space-based PNT	• Reduce susceptibility to jamming and spoofing through signal and constellation diversity
	System	
	• Resilient user equipment	• Harden against interference; detect, isolate, and contain threats to prevent cascading operational effects

Hazard class	Resilience levers	Resilience objective
Supply chain (escalating in grey zone)	**Policy**	
	• Sovereign or domestically controlled PNT components • Consideration of domestic manufacturing	• Reduce risk / exposure to coercion and disruption of PNT supply chain • Limit reliance on high-risk single-source PNT dependencies
	Technology	
	• Sovereign timing distribution and ground segment control	• Assure access to critical PNT services under contested or degraded supply conditions
Personnel (increasing in competition)	**Governance**	
	• National and institutional governance and coordination measures	• Reduce risk of insider threat through controlled access and oversight of critical PNT functions
	System	
	• Distributed architectures	• Reduce and dilute the impact of malicious insider activities through redundancy and separation of systems

In terms of technology options, Table 34 highlights the need for a deliberately layered and diversified PNT profile for Australia. Multi-layered space-based PNT, terrestrial systems, onboard sensors, and timing holdover capabilities each provide distinct alternatives, but their resilience value is greatest when combined as part of an integrated system-of-systems. The following recommendations focus on priority actions, targeted validation activities, and enabling measures where further evaluation and early implementation would materially strengthen Australia's PNT resilience objectives.

6.2 Space-based PNT Options for Australia

Australia's future PNT architecture should continue to treat space-based signals as the foundational layer for national and Defence PNT, while recognising that GNSS alone is insufficient to assure access in contested environments. Australia's priorities should therefore be to strengthen and diversify space-based PNT dependencies through a multi-layered satellite architecture that gives Defence greater confidence that PNT will be available when it is most needed.

ADF recognises that GPS can be denied through jamming and spoofing and is already pursuing upgrades across platforms and systems. The options below are presented as a scan of available approaches rather than a recommendation. Further technical assessment and cost-benefit analysis would and should be required to identify preferred pathways for Australia. It is then treated as a strong recommendation of this study to deliver a set of clear requirements and architectures for Australia to deliver a resilient PNT capability. This has in the past been delivered by work from the UK [112], or been first indirectly proposed through Radio Navigation Plan, such as that in Europe [113].

6.2.1 GNSS constellation diversity

Australia should continue to consider multi-constellation GNSS as its baseline source, including GPS, Galileo, as well as regional constellations such as Japan's QZSS, India's NaVIC, and the future South Korean KPS. However this may be more feasible for civilian sectors compared to Defence, for reasons of maintaining compatibility across Five Eyes systems. This diversity can improve resilience against natural hazards and non-kinetic disruptions.

6.2.2 Prioritise sovereign control of augmentation and ground infrastructure

In the absence of a sovereign GNSS constellation, control of the GNSS augmentation layer and ground segment is a practical lever for sovereignty. Continued government investment into SouthPAN (reference stations, uplinks and processing hubs) and integration into Defence systems should not be overlooked, bearing in mind that SouthPAN would be susceptible to the same vulnerabilities that affect GNSS, i.e. jamming, spoofing, meaconing, etc. This scenario is considered current state and is shown graphically in Figure 9.

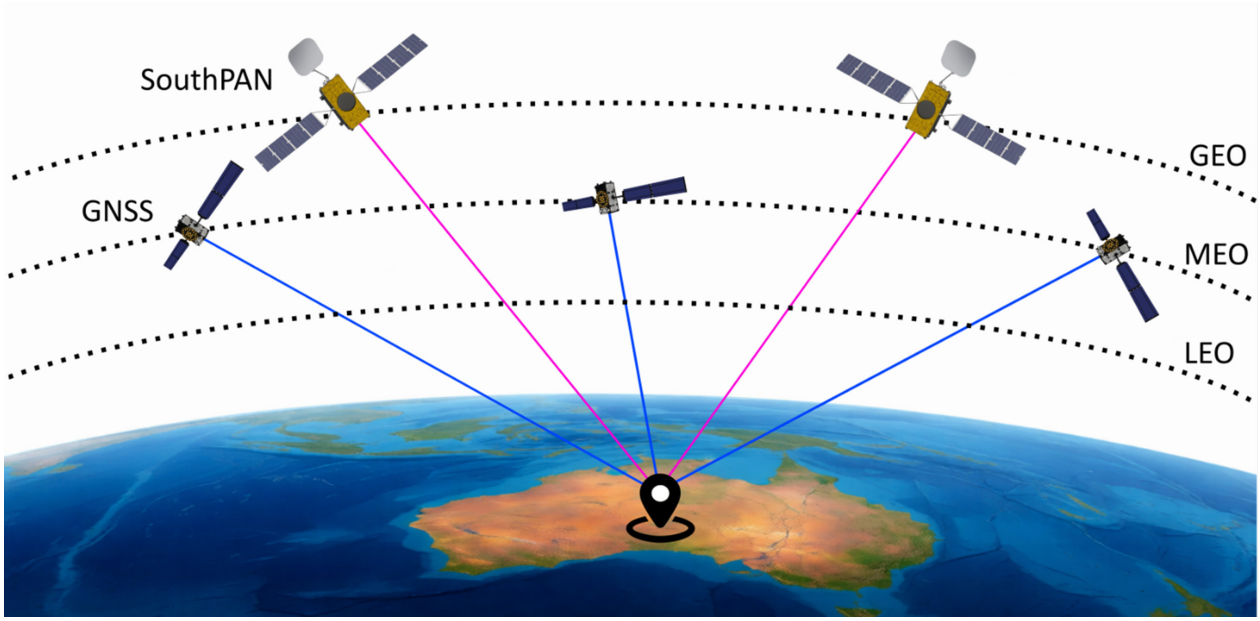

Figure 9: Current state of space-based PNT in Australia.

6.2.3 LEO PNT as part of a distributed, multi-layered space architecture

LEO PNT in Australia remains at an early stage of development, but could be pursued as a complementary resilience layer to GNSS. Stronger space-to-earth signals, rapid geometry changes, and the potential for integration with communications services make LEO-based systems attractive for contested environments.

LEO PNT can be achieved through various ways. One such way is to launch a dedicated constellation, which is the approach taken by an increasing number of countries including the United States, the European Union, Japan, China, the United Arab Emirates, Türkiye, India, and the Republic of Korea (see Section 5.1.2.1). However, launching a dedicated PNT constellation is an expensive option. There are various other ways Australia could achieve LEO PNT, which are summarised below:

- Selective sovereign contributions (e.g., payloads or partial constellations) integrated with a partner nation's system.
- Partnering with allied or commercial LEO PNT providers for services.
- Undertake trials and demonstrations to evaluate the feasibility and scalability of integrating LEO PNT signals into GNSS-primary systems.
- Leveraging LEO systems deployed for other primary applications, such as air traffic management as sources of PNT signals [114].

These options align with Australia's growing space sector, enable more flexible deployments, and provide improved access to resilient signals without the costs of sovereign infrastructure. Figure 10 shows the space-based PNT landscape including a dedicated LEO PNT service for Australia.

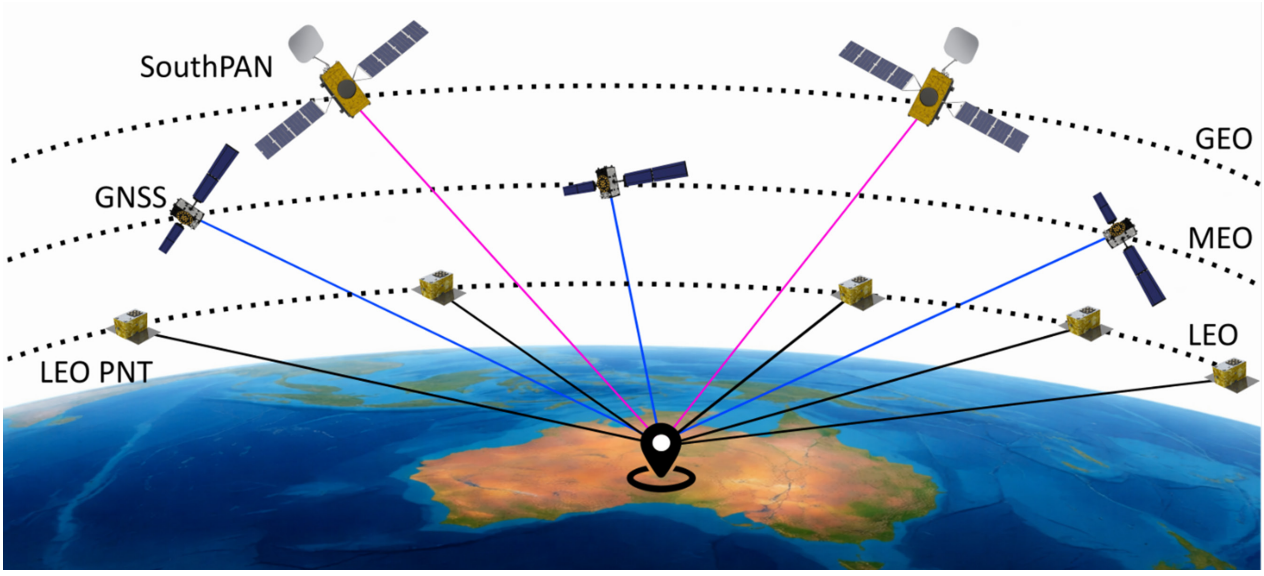

Figure 10: Space-based PNT landscape including LEO PNT.

6.2.4 Apply space-based maritime PNT service in coastal areas

Space-enabled maritime PNT, including satellite-supported VDES-R mode, should be considered a domain-specific resilience layer rather than a national solution. Partnering with AMSA to trial VDES-R for ports and naval operations would allow Defence to assess its value in mitigating GNSS disruption in coastal and maritime environments.

This is especially relevant where RF interference threats are acute. In addition, integrating VDES with terrestrial coastal transmitters could support hybrid R-Mode PNT solutions, offering both communications and resilient positioning to vessels operating in Australian waters. This is shown graphically in Figure 11 below.

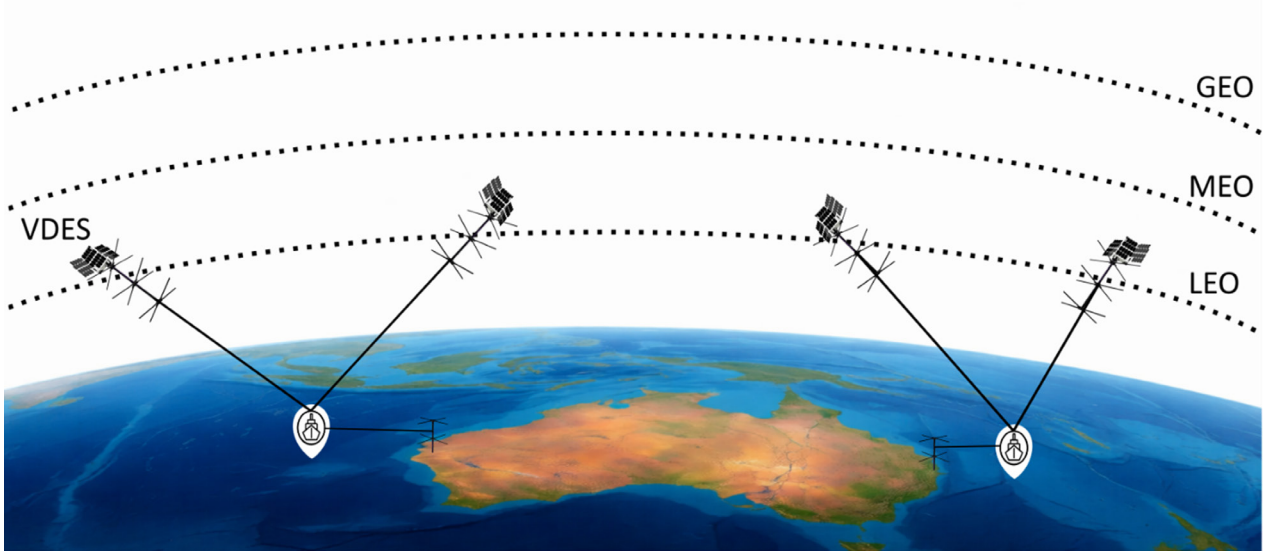

Figure 11: Conceptual VDES-R service for Australian coastal waters.

The maritime domain is particularly well suited to VDES. Vessel operations are geographically constrained, safety-critical, and already subject to coordinated regulation and infrastructure deployment along the coastline. This allows new PNT services to be introduced incrementally, trialled operationally, and evaluated against clear performance and safety metrics. For Defence, maritime trials also offer an opportunity to assess interoperability between civil and military users, and to understand how domain-specific PNT services could be integrated into wider joint operations without implying a national-scale deployment.

6.2.5 Joint PNT and SATCOM

Integrating PNT and SATCOM could provide a force multiplier within a layered space architecture. This could include leveraging Defence and commercial SATCOM assets for GNSS integrity monitoring, secure dissemination of PNT corrections, or direct provision of timing signals. This approach is in line with emerging international practice while supporting Defence objectives for assured access to communications and PNT in contested environments. Additionally, partnering with a satcom provider would enable Australia to access resilient, dual-use capabilities without bearing the full cost of deploying new infrastructure [115]. This option is shown in Figure 12 below.

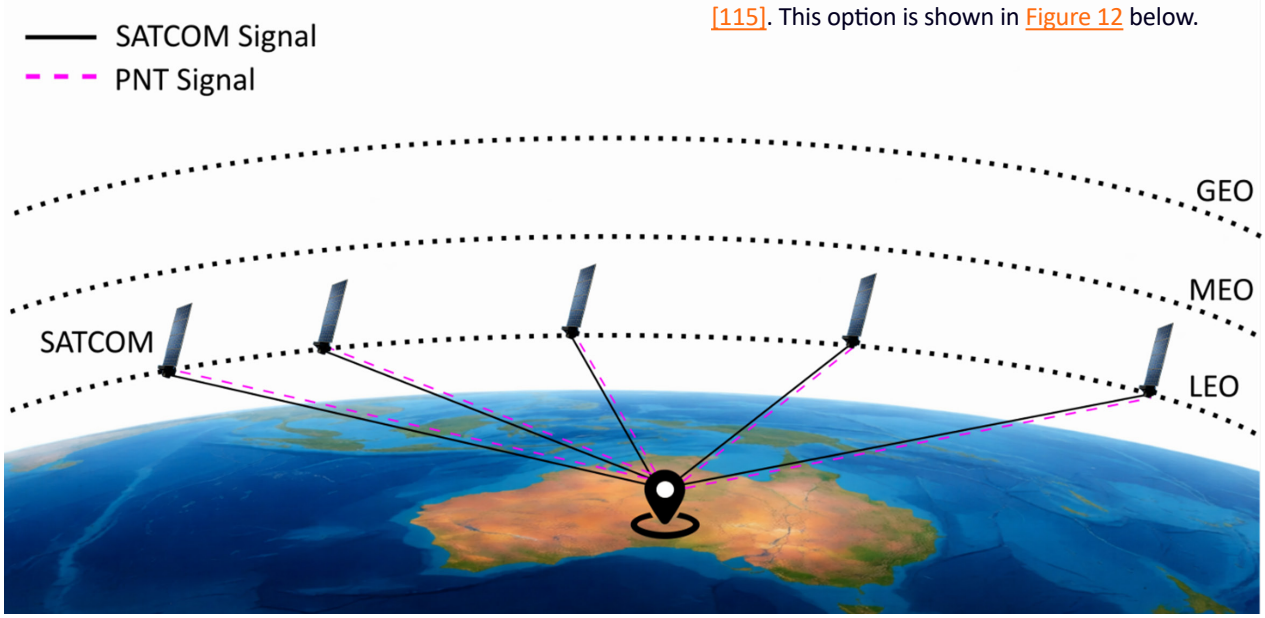

Figure 12: Conceptual Fused PNT and SATCOM service for Australia.

In this context, joint PNT and SATCOM architectures should be viewed as an enabling integration approach, rather than as a standalone PNT replacement. Their value lies in combining assured communications with PNT-related functions such as integrity monitoring, control messaging, and resilient dissemination of timing or correction data. For Australia, the priority is therefore to understand where such integration can deliver genuine resilience benefits, how dependencies on shared space assets are managed, and what governance arrangements are required when relying on dual-use commercial services in contested environments.

6.2.6 PNT as a Service

PNT as a service could provide another option for an alternative PNT solution, especially due to the fact that it does not require the launch of its own satellite constellation. By setting up a number of reference and monitoring stations around the country, Defence could utilise signals from different satellites in LEO and GEO orbits to achieve a PNT capability that is operationally independent of GNSS. This option is shown in Figure 13.

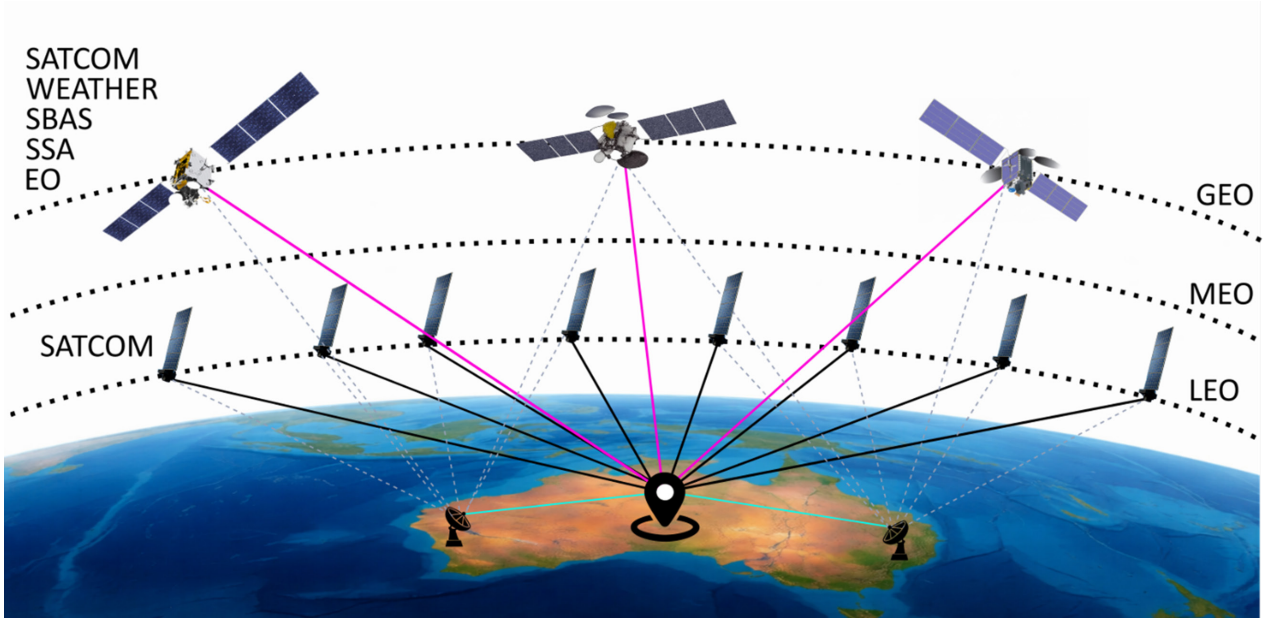

Figure 13: Conceptual PNT as a service framework for Australia including ground segment.

A defining feature of PNT-as-a-Service is the ground segment, consisting of reference and monitoring stations which observe space-based signals of opportunity from selected satellites across multiple frequency bands and orbits, estimate signal characteristics, and publish corrections or timing data to users via secure data services [63, 64].

6.3 Terrestrial-based PNT options

Terrestrial-based PNT systems could be considered as a critical resilience layer within Australia's future PNT architecture by providing continuity of PNT services when space-based systems are disrupted. Terrestrial-based systems are at this stage unlikely to fully replace GNSS or SouthPAN. Instead their role would be to limit adverse impacts to missions and operations, and provide continuity under interference, outages, or localised degradation. This is especially so for natural, physical, and EM hazards. This could mean deploying a backbone terrestrial capability such as eLoran, supported by additional technologies which could include R-Mode, local terrestrial pseudolite networks, fibre-based timing, and 5G/3GPP broadcast. Alternatively to radio-over-the-air time transfer, cable-based time synchronisation could be achieved through existing or developing new fibre optic networks across Australia.

The maritime domain represents an applicable use case for terrestrial PNT in Australia due to:

- Safety-of-life implications
- Concentration of existing PNT infrastructure
- Concentration of infrastructure enabled by PNT
- Exposure to GNSS disruption via interference

6.3.1 eLoran

In the maritime domain, terrestrial systems are already well understood as part of a layered navigation framework. eLoran is the only option that provides continent-scale, wide-area coverage, with long-wave signals able to reach hundreds of kilometres offshore. It can ensure continuity of timing and navigation for shipping when GNSS is unavailable. Additionally, it can provide a different signal type that is highly resistant to jamming, thereby reducing reliance on space-based PNT during disruption.

Some of these concepts are illustrated graphically below. Note, the following maps are conceptual only and are based on the attainable geometric ranges of each technology. They are intended to demonstrate the relative coverage characteristics and layering potential of different terrestrial PNT classes. They do not represent endorsed network designs, validated geometries or costed deployment options. Figure 14 shows a configuration of six eLoran sites spread around Australia at distances of roughly 900km, which would be sufficient to support national timing coverage.

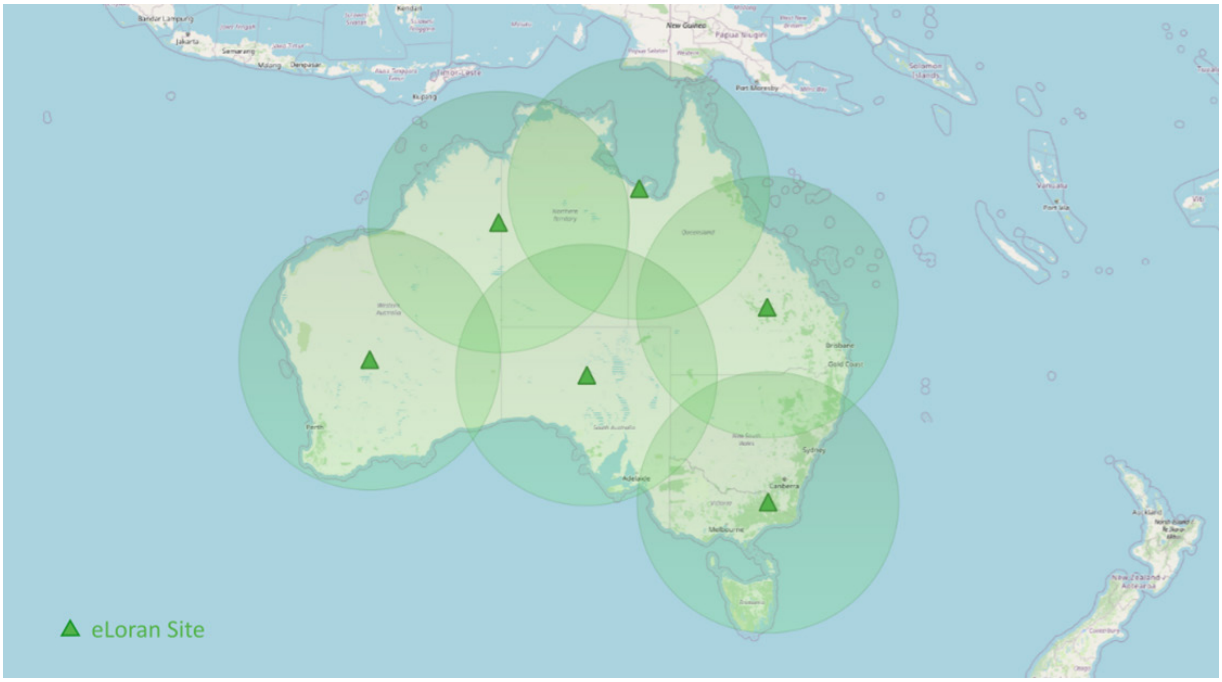

Figure 14: Notional eLoran-style terrestrial timing coverage to support national resilience.

It is envisaged that the network could be extended to around 10 stations to cover Australia for positioning and navigation services, however, proper modelling will need to be carried out to design the network, which is outside the scope of this report.

6.3.2 Coastal Ranging Mode systems

Closer to the coast, MF or AIS/VDES R-Mode could offer a complementary service by converting legacy AMSA DGPS beacon sites into R-Mode transmitters. These sites, decommissioned in 2020, could be revived and upgraded to broadcast continuous, phase-stable ranging signals that enable position fixes up to 300 nautical miles offshore [116].

Figure 15 shows the conceptual design of the terrestrial R-Mode network based on the former AMSA DGPS network [117]. The circles represent 300 NM (or 550 km) radius of each station, which is the practical mode of R-mode transmission [74]. It can be seen that if the network is to be revived, it will cover most of the Australian coastline, with a few gaps in the north, south and west, which could be infilled by 4-5 extra stations for full coverage. Figure 16 then illustrates the combination of eLoran and R-Mode.

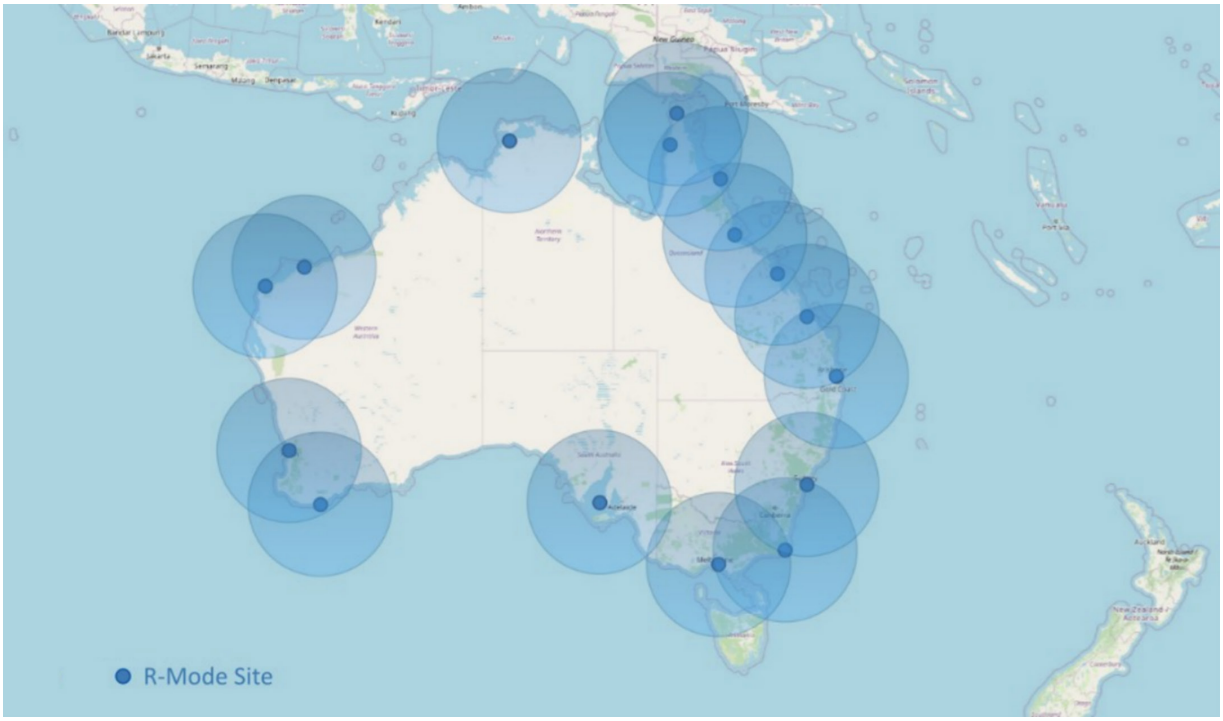

Figure 15: Conceptual R-mode network based on the former AMSA DGPS network.

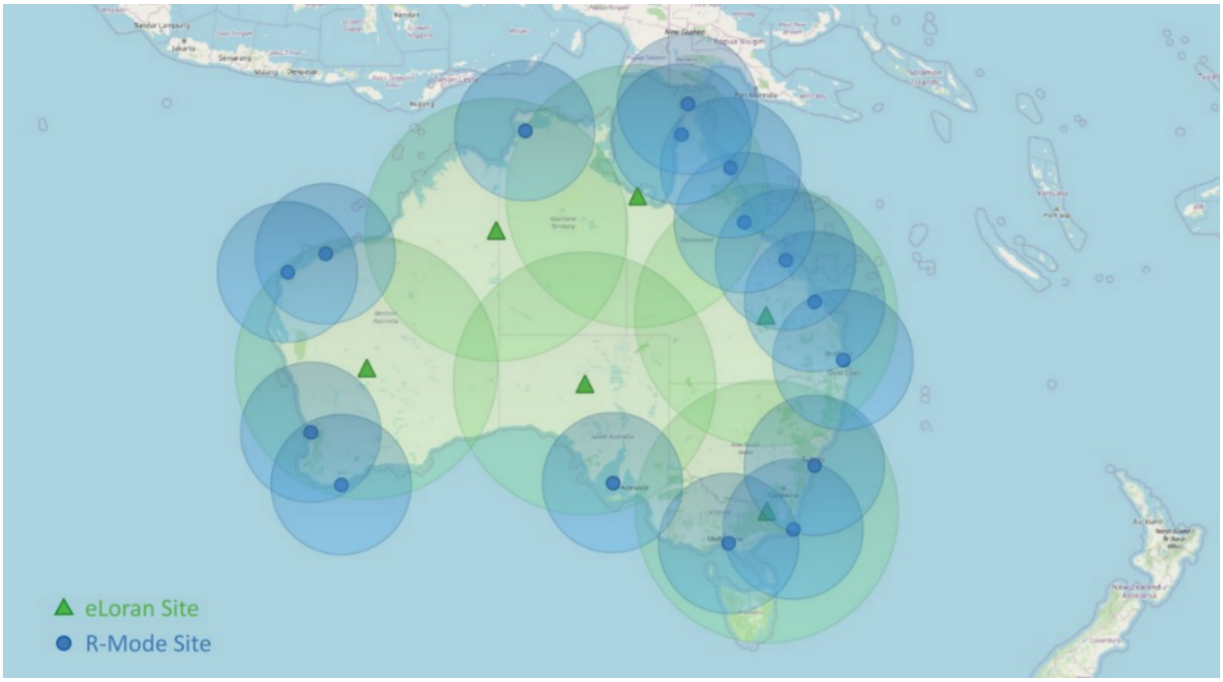

Figure 16: Conceptual combined eLoran and R-mode network.

6.3.3 Local-area Pseudolite networks

Local-area terrestrial pseudolite positioning networks, can deliver high-accuracy PNT services at key ports and offshore facilities. Locata is an example of this class of technology that is currently used at the White Sands Missile Range in the US during jamming and spoofing testing [118].

Figure 17 shows how conceptual networks could be deployed around key defence installations in Australia, namely HMAS Stirling in Perth and HMAS Coonawarra in Darwin. A small number of strategically located transmitters could provide coverage supporting coastal navigation, remote area timing, critical infrastructure synchronisation and defence activities. Existing broadcast or defence infrastructure could be leveraged to reduce deployment costs. eLoran can also be integrated with local-area networks, combining long-range, high-power coverage with the high-accuracy, localised performance.

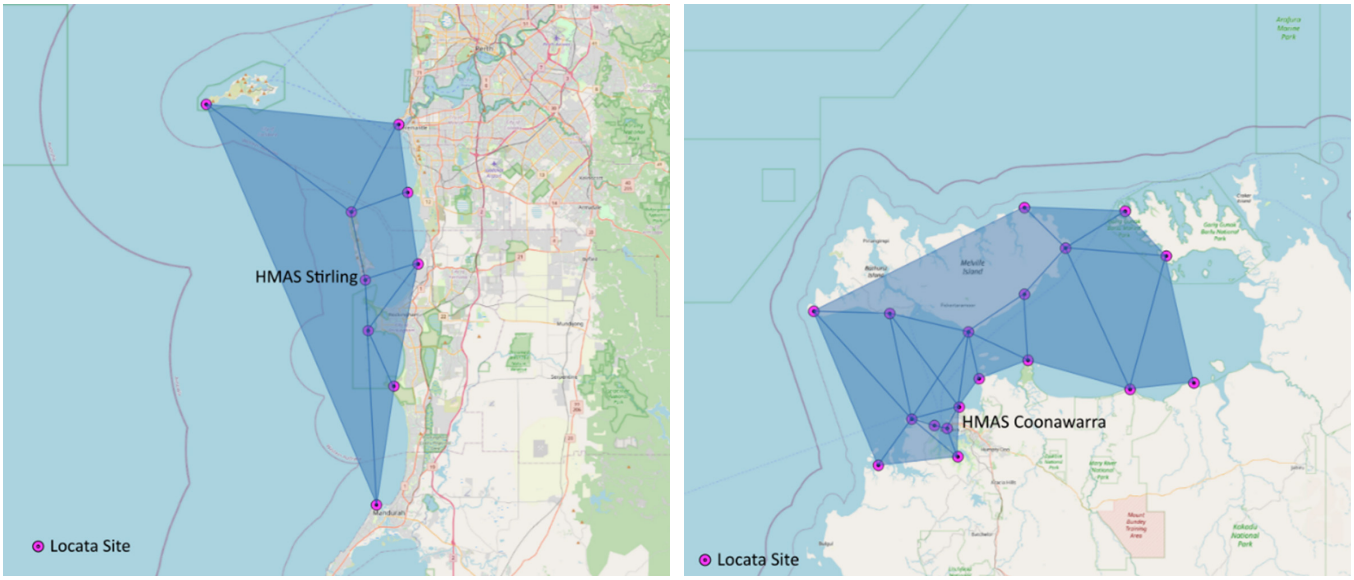

Figure 17: Conceptual pseudolite networks at HMAS Stirling and HMAS Coonawarra Naval Bases.

6.3.4 Fibre-Based Time Transfer

Fibre-based time transfer can provide authoritative time distribution between trusted reference clocks at strategic locations, such as data centres, headquarters, and sensor fusion nodes. It can also support holdover management and recovery by maintaining synchronisation between distributed local clocks during GNSS outages. Utilising dark fibre (installed but unlit optical fibre with no active transmission equipment) in the existing networks can provide complementary time transfer for defence and |critical infrastructures.

In the Australian context, several fibre-optic backbones span major metropolitan centres and extend into key regional corridors. One example of a fibre-optic network is AARNet (Figure 18), the national research and education network that interconnects universities, research institutions, government agencies, and major scientific facilities across the country.

Figure 18: National AARNet Fibre Network [119].

Access to dark fibre fundamentally changes the resilience characteristics of terrestrial time transfer. By enabling physically controlled, point-to-point optical paths, dark fibre allows Defence to establish timing links that are operationally independent of shared commercial packet-switched networks and logically decoupled from satellite-based timing services.

6.3.5 Broadcast Radio–Based PNT (AM/FM)

Australia's existing AM and FM broadcast radio networks present a potential opportunity to explore complementary terrestrial PNT capabilities by leveraging widely deployed national infrastructure.

With almost 300 commercial AM and FM broadcast stations distributed across the country, a subset of those could be equipped with appropriate PNT augmentation hardware to support limited positioning or timing services based on multilateration or time-based techniques (conceptual design shown in Figure 19).

However, the suitability of AM and FM broadcast systems for operational PNT use remains unproven. As such, any consideration of broadcast radio for PNT should be treated as an exploratory or complementary option, requiring systematic testing, validation, and governance assessment before it could be considered as part of a resilient national PNT architecture. If validated, such an approach could offer a cost-effective supplement to other terrestrial and space-based PNT layers rather than a standalone solution.

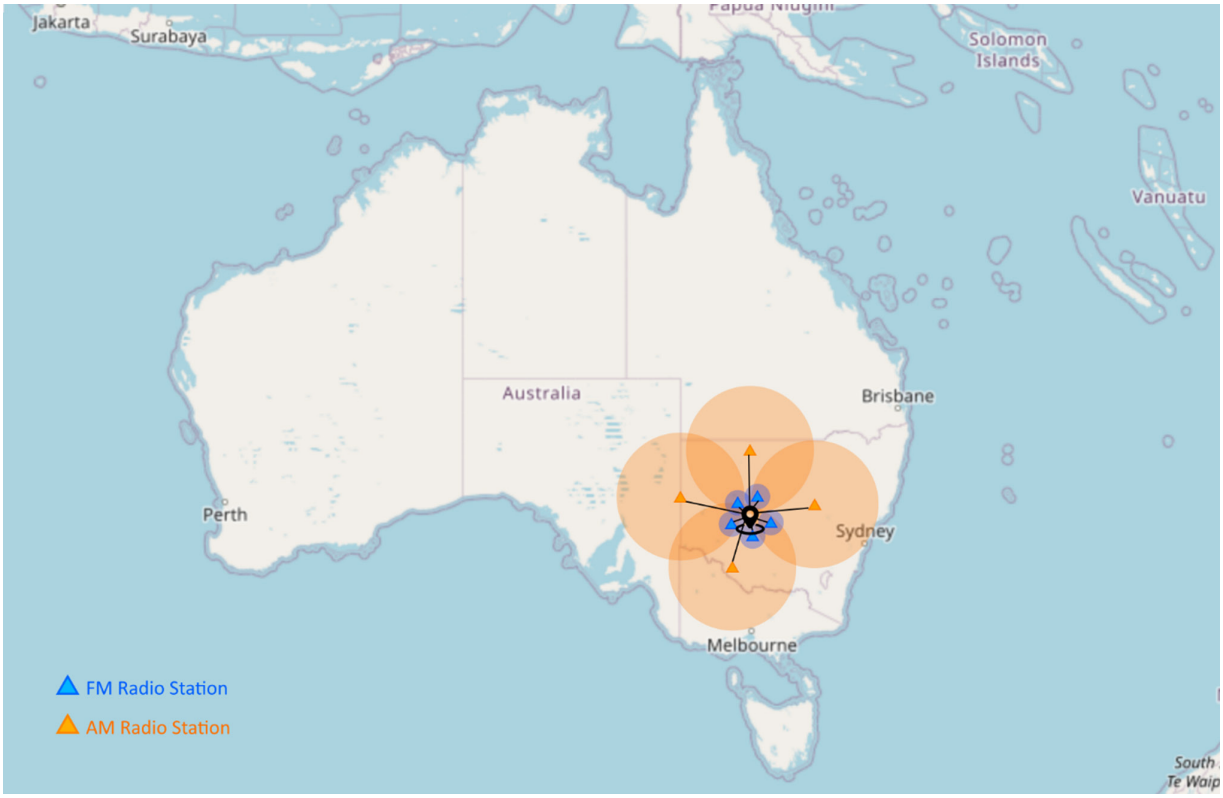

Figure 19: Conceptual position estimation using AM and FM radio broadcast.

Terrestrial-based PNT systems collectively offer Australia practical means to reduce dependence on space-based signals. Some of the illustrations above demonstrate single solution approaches. However, realistically a layered terrestrial approach combining wide-area, coastal, and localised capabilities would enable Defence and civil authorities to sustain essential PNT functions without going down the pathway of a single monolithic solution.

6.4 Chapter Summary

Resilient PNT cannot rely on any single technology or source but instead requires a layered system-of-systems approach that combines satellite services with terrestrial networks and onboard capabilities. This layered approach aligns with international best practice. The United States Department of Transportation has concluded that national PNT resilience is best achieved through the use of a plurality of diverse and mature technologies, rather than reliance on a single system [120]. In particular, it identifies complementary use of space-based PNT services, terrestrial broadcast signals, and fibre-supported time distribution to transmitting and control infrastructure as a robust foundation for resilient national PNT capability. This architectural diversity reduces common-mode failure risk and supports continuity of essential services under a wide range of disruption scenarios.

Space-based solutions continue to play a central role in resilient PNT architectures, particularly where wide-area coverage and global consistency are required. In addition to GNSS, emerging space-based approaches such as LEO PNT, hybrid-constellation use, signal authentication, and alternative orbital regimes can provide increased diversity within the space domain itself. While these approaches remain subject to space-segment and RF threats, they can improve robustness through redundancy, frequency diversity, and faster recovery when integrated as part of a layered system-of-systems architecture.

Terrestrial timing solutions, including fibre-based time transfer, offer a physically independent complement to satellite timing and can enhance robustness where access, governance, and security requirements permit. While such infrastructure does not replace satellite PNT, it can play an important supporting role in maintaining synchronisation, enabling cross-checks, and supporting recovery during GNSS disruptions.

The following recommendations are made:

- Define a nationally-coordinated threat-driven and risk-based requirements for PNT resilience.
- Undertake feasibility studies of PNT architectures to meet these requirements.
- Review existing policy, regulatory, and standards frameworks to support resilient PNT outcomes.
- Develop an Australian PNT Strategy to guide Australia's future PNT capability.

7 CONCLUSION

Threats to PNT can arise as both overt and less obvious forms. Many are not immediately identified as PNT issues, instead presenting as industrial, economic, or geopolitical challenges. However, events that appear unrelated to PNT can still degrade the availability and integrity of PNT information. This can happen in cooperative, contested, and conflicted environments. When this information is compromised, impacts can cascade across operational, assurance, and safety functions across entire sectors.

Examining PNT threats through a hazards-based lens helps clarify how different threats arise and interact. Considering these threats across the cooperation-competition-conflict spectrum then aligns these threats with national and defence frameworks, for understanding and responding to disruption. PNT resilience therefore begins with awareness of what constitutes a threat. It is then reinforced through situational awareness enabled by detection and response. Resilience is ultimately achieved through an integrated mix of governance, industrial policy, and system hardening, supported by appropriate technological solutions and architectures.

While this report gives particular attention to technology options, it shows that PNT resilience is achieved by applying a broader set of integrated measures and capabilities. Different hazard classes and stages of competition place emphasis on different resilience levers, and which requires complementary roles across Defence and civil government. Defence has a central function in assuring PNT for mission-critical operations, and there is a clear though non-exclusive national leadership role for PNT technology uplift and architectural resilience. Civil government in turn plays a leading role in designing industrial and economic policy settings, and cross-sector coordination to manage systemic and nationally-shared PNT risks. Accordingly:

- Space- and terrestrial-based PNT capabilities can reduce Australia's PNT vulnerability to natural and physical hazards that threaten PNT across the competition spectrum.
- Well-considered industrial and economic policies are central to managing supply chain hazards.
- System and user equipment hardening presents an initial line of deterrence and defence against cyber, information and EM hazards.
- Finally, strong national and institutional governance, complemented by detection mechanisms and distributed PNT architectures, is critical to mitigated personnel hazards.

Given Australia's place in the Indo-Pacific region, these measures would provide a layered approach to securing trusted and resilient PNT in an increasingly contested environment. ANCHOR makes the following recommendations:

Recommendations

1. **Define nationally-coordinated threat-driven and risk-based requirements for PNT resilience.**
   Establish clear, nationally-consistent requirements that can specify the level of resilience required to maintain essential services and national security functions. These requirements should be based on identified PNT threats, and both civil and Defence operational outcomes.
2. **Undertake feasibility studies of PNT architectures to meet these requirements.**
   Evaluate a range of complementary and layered PNT architectures to determine their technical feasibility, cost, scalability, and ability to meet both civil and Defence PNT resilience requirements.
3. **Review existing policy, regulatory, and standards frameworks to support resilient PNT outcomes.**
   Assess how current policies, regulations and standards governing critical infrastructure sectors can be leveraged, adapted, or amended to accelerate adoption of resilient PNT architectures and best-practices. Ensure these frameworks also support Defence assurance and interoperability requirements.
4. **Develop an Australian PNT Strategy to guide Australia's future PNT capability.**
   Create a whole-of-nation PNT Strategy that provides strategic direction for Australia's future PNT capability. The Strategy should clarify roles and responsibilities across Defence, civil agencies, and industry, and align stakeholders towards a coordinated resilient PNT capability for Australia. The Strategy should also make steps towards outlining implementation roadmaps and regulatory instruments, such as a Radio Navigation Plan.

APPENDIX A:
CONSEQUENCE SCORING

The consequence of each hazard class was assessed across the competition spectrum. The hazard classes are:

- Cyber, Information, Electromagnetic
- Personnel
- Supply Chain
- Physical
- Natural

The phases of the competition spectrum are Cooperation, Competition, Conflict.

Associated examples within the hazard-competition spectrum threat matrix have been assigned consequence scores based on critical factors (presented in Section 3.3.1). The raw results are presented here, while consolidated results are presented in text in Section 3.3.2 Consequence Assessment Results.

Cyber, Information, EM

Cooperation phase examples:

- Pre-operational testing identified error in Australia's SouthPAN correction data.
- White hat testing of timing-dependent SCADA systems as part of audit and compliance.
- Simulation and testing of interference scenarios as part of assured PNT product R&D.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 2

Competition phase examples:

- GNSS jamming in the South China Sea affecting ports, maritime operations, aviation.
- Living off the land cyber intrusions into PNT systems (space, ground, user segment) that are difficult to detect and attribute.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 2

Conflict phase examples:

- Deliberate GPS spoofing conducted by state actors during open conflict (e.g. in Eastern Europe, Middle East)

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 3.67

Personnel

Cooperation phase examples:

- Temporary GNSS outage caused by authorised on-site ground segment maintenance
- Navigating to sensitive physical sites via connected in-vehicle navigation systems.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 2.33

Competition phase examples:

- Use of personnel to undertake benign PNT activities that may be re-purposed for dual-use or illicit activities.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 3.67

Conflict phase examples:

- Sabotage or insider interference at a GNSS ground station, intentionally disrupting services for operational advantage during conflict.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 3.66

Supply chain

Cooperation phase examples:

- Mergers and acquisitions of PNT device suppliers and manufacturers.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 1

Competition phase examples:

- Introducing compromised components into commercial or government GNSS supply chains, causing faulty hardware or software bugs in the space, ground and user segments.
- Restricting supply of critical components for PNT systems to create dependency.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 3.33

Conflict phase examples:

- Denial of access to critical components for PNT systems to deliberately exacerbate consequences of PNT disruptions to critical infrastructure.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 4

Physical

Cooperation phase examples:

- Surveys and testing of physical security and risk management of PNT infrastructure and assets.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 1

Competition phase examples:

- "Accidental" damage of subsea cables relaying timing data.
- ASAT tests; in-orbit rendezvous operations in proximity to GNSS satellites.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 2.33

Conflict phase examples:

- Physical destruction of GNSS ground network due to hostilities.
- Missile strikes on energy infrastructure causing flow-on impacts on GNSS ground network operations.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 5

Natural

Cooperation phase examples:

- Unpredictable space weather or natural disaster events causing temporary degradation of PNT services.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 3

Competition phase examples:

- Exploitation of PNT vulnerabilities through other means (e.g cyber, physical, personnel) during windows of opportunity caused by natural hazards.
- Offering PNT assistance during crises framed as cooperation, but which creates debt and dependencies for the host, with the intent of expanding soft power in the region.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 4

Conflict phase examples:

- Natural hazards amplify the impacts of PNT disruptions in conflict zones.

Consequence (Score)	Critical infrastructure	Defence situational awareness	Public perception and safety
Severe (5)	National coordination and communication disabled. Enterprise / social systems not functioning. National governance mechanisms fail. National security severely compromised.	C5ISR disabled across all Defence domains. No situational awareness; mission execution impossible. Likelihood of multiple concurrent threats.	Widespread loss of life. Loss of social cohesion. Defence required to restore civil unrest.
Major (4)	National coordination degraded. Enterprise / social systems overwhelmed. National governance mechanisms degraded.	C5ISR disabled in 3-5 Defence domains. Mission objectives cannot be realised. National security compromised; significant structural adjustment required.	High public fear and insecurity. Loss of confidence in government response. Serious casualties and fatalities. Defence required to restore civil unrest.
Moderate (3)	Business-as-usual coordination not possible. Noticeable degradation of enterprise / social systems. National governance mechanisms partially impaired.	Grey-zone threats not contained. C5ISR degraded across 3-4 domains. Reduced situational awareness. Mission risk elevated.	Sustained public concern. Potential for several casualties. Government response closely scrutinised.
Minor (2)	Coordination hindered but workarounds available. Minor degradation to enterprise / social systems. Localised governance and decision-making impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded; still functional via alternatives. Minor mission impact in a grey-zone context.	Increased public interest but limited concern. Minor casualties possible, no fatalities.
Insignificant (1)	Negligible impact. Enterprise / social systems cope without major change. Decisions escalated through normal governance.	No meaningful impact on C5ISR or operations. Situational awareness maintained.	Public concern is minimal. Only minor injuries treatable onsite. No long term effects.

Average consequence score: 5

APPENDIX B:
PNT TECHNOLOGY TEST CAMPAIGNS

A number of test campaigns have been carried out to test the various alternative and complementary PNT technologies by the Department of Transportation (DOT) Volpe Centre in the US and the Joint Research Centre (JRC) in Europe. These are summarised below.

In 2021 US DOT has carried out an evaluation campaign to test complementary PNT technologies from eleven vendors. Table 35 provides the information on each vendor's technology, in particular whether it is space-based or terrestrial, and whether it can do positioning, navigation or timing, as well as the technical details on which frequency range is used. Comprehensive results of the testing can be found in the published report titled *Complementary PNT and GPS Backup Technologies Demonstration Report* [121].

Table 35: DOT Complementary PNT and GPS Backup Technologies Campaign 2021.

DOT Complementary PNT and GPS Backup Technologies Campaign 2021					
Vendor	**Country**	**PNT Service**	**Space / Terrestrial**	**Technology**	**Frequency (MHz)**
Echo Ridge	USA	P	Space	LEO commercial S-band	2,483.5 – 2,500
Hellen Systems	USA	P,N,T	Terrestrial	eLoran	0.090 – 0.110
NextNav	USA	P,N,T	Terrestrial	UHF terrestrial RF	920 - 928
OPNT	Netherlands	T	Terrestrial	Time transfer fibre	N/A
PhasorLab	USA	P,N,T	Terrestrial	802.11 terrestrial RF	2400
Satelles	USA	P,N,T	Space	LEO commercial L-band	1,616 – 1,626.5
Serco	USA	P,N,T	Terrestrial	MF R-mode	0.2835 – 0.325
Seven Solutions	Spain	T	Terrestrial	Time transfer fibre	N/A
Skyhook Wireless	USA	P,N	Terrestrial	802.11 terrestrial RF	900, 2,400, 5,000
TRX Systems	USA	P,N	Terrestrial	UWB & IMU map matching	3,100 – 5,000
UrsaNav	USA	P,N,T	Terrestrial	eLoran	0.090 – 0.110

The Joint Research Centre under the European Commission, has carried out a similar study in 2023, where it evaluated PNT technology from seven different vendors, as detailed in Table 36.

Table 36: JRC Alternative PNT Technologies Evaluation Campaign 2023.

JRC Alternative PNT Technologies Evaluation Campaign 2023					
Vendor	**Country**	**PNT Service**	**Space / Terrestrial**	**Technology**	**Frequency (MHz)**
OPNT	Netherlands	T	Terrestrial	Time transfer fibre	N/A
Safran[2]	France	T	Terrestrial	Time transfer fibre	N/A
SCPTime	France	T	Terrestrial	Time transfer networks	N/A
GMV	Spain	T	Terrestrial	Time transfer fibre, networks	N/A
Satelles	USA	P,N,T	Space	LEO commercial L-band	1,616 – 1,626.5
Locata	Australia	P,N,T	Terrestrial	Timeloc, time transfer fibre	2,400
NextNav	USA	P,N,T	Terrestrial	UHF terrestrial RF	920 - 928

[2] Previously Seven Solutions.

The results of the evaluation campaign are detailed in the published report titled Assessing Alternative Positioning, Navigation, and Timing Technologies for Potential Deployment in the EU [80].

In 2025, US DOT has carried out another evaluation campaign, specifically targeting vendors with high Technical Readiness Level (TRL) solutions. This time, nine technology vendors underwent the testing and evaluation campaign, as detailed in Table 37 [111].

Table 37: DOT Complementary PNT and GPS Backup Technologies Campaign 2025.

DOT Complementary PNT and GPS Backup Technologies Campaign 2025					
Vendor	**Country**	**PNT Service**	**Space / Terrestrial**	**Technology**	**Frequency (MHz)**
Hoptroff	UK	T	Terrestrial	Time transfer fibre	N/A
NAL Research Corp	USA	P,N,T	Space	LEO commercial L-band	1,616 – 1,626.5
Locata	Australia	P,N,T	Terrestrial	Timeloc, time transfer fibre	2,400
Parsons[3]	USA	T	Space	LEO commercial S-band	2,483.5 – 2,500
Carahsoft	USA	P,N	Terrestrial	Camera/Map Matching	N/A
Safran[4]	France	T	Terrestrial	Time transfer fibre	N/A
NextNav	USA	P,N,T	Terrestrial	UHF terrestrial RF	920 - 928
Microchip	USA	T	Terrestrial	Time transfer fibre	N/A
Tern AI	USA	P,N	Terrestrial	Sensor/Map Tracking	N/A

At the time of writing, the results of this campaign have not been published yet and are expected to be published in early 2026.

In addition to the DOT and JRC trials, the UK's Maritime Resilience and Integrity in Navigation (MarRINav) study also examined resilient PNT solutions for the maritime domain. Unlike the evaluation campaigns conducted by DOT and JRC, MarRINav did not involve live technical trials of vendor systems. Instead, it provided a comprehensive description of candidate resilient PNT technologies within a maritime system-of-systems framework. The report assessed their potential roles, integration with dead reckoning and GNSS, and implications for UK critical maritime infrastructure, but its analysis was primarily conceptual and architectural rather than experimental [122]. The technologies evaluated in the MarRINav study are shown in Table 38 below.

Table 38: MarRINav Resilient PNT Technology evaluations for maritime.

MarRINav Technology Evaluation 2020			
Technology	**PNT Service**	**Space / Terrestrial**	**Frequency (MHz)**
eLoran	P,N,T	Terrestrial	0.090 – 0.110
VDES R-Mode	P,N,T	Terrestrial	0.3 - 3
Radar Absolute Positioning	P,N	Terrestrial	9,000 (X-band), 3,000 (S-Band)
Satelles STL	P,N,T	Space	1,616 – 1,626.5
Locata	P,N,T	Terrestrial	2,400
Tern AI	USA	P,N	Terrestrial

[3] Previously Echo Ridge.
[4] Previously Seven Solutions.

REFERENCES

1. Proctor, A. (2022). How to achieve PNT system resilience – a structured approach. *RethinkPNT White Paper*. Available at: https://rethinkpnt.com/projects-and-papers/ (Accessed: 25 January 2026).
2. NLA International (2025a). *Supporting the UK Public Sector in PNT Awareness, Research and Knowledge (SPARK). Part 1 – Existing and Emerging PNT Services*. NLA International.
3. FrontierSI (2025a). *Assessing PNT Disruptions and Their Impacts on Defence*. Available at https://frontiersi.com.au/assessing-pnt-disruptions-and-their-impacts-on-defence (Accessed: 25 January 2026).
4. FrontierSI (2025b). *Beyond GPS: Charting Australia's PNT Future in an Uncertain World*. Available at https://frontiersi.com.au/wp-content/uploads/2025/06/FrontierSI_Beyond-GPS_Charting-Australias-PNT-Future_Report.pdf (Accessed: 25 January 2026).
5. Critical Infrastructure Security Centre (CISC) (2025). *Guidance for the Critical Infrastructure Risk Management Program*. Canberra: Department of Home Affairs. Available at: www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf (Accessed: 25 January 2026).
6. Critical Infrastructure Security Centre (CISC) (2024). *Factsheet for Critical Infrastructure: Positioning, Navigation and Timing*. Canberra: Department of Home Affairs. Available at: www.cisc.gov.au/resources-subsite/Documents/pnt-factsheet.pdf (Accessed: 25 January 2026).
7. Cyble Research & Intelligence Labs (2024). *GhostSec targeting satellite receivers*. Available at: https://cyble.com/blog/ghostsec-targeting-satellite-receivers/ (Accessed: 25 January 2026).
8. Greenberg, A. (2022). A mysterious hack crippled satellite internet across Ukraine. *Wired*, 1 March 2022. Available at: www.wired.com/story/viasat-internet-hack-ukraine-russia/ (Accessed: 25 January 2026).
9. Beutler, G., Dach, R., Hugentobler, U., Montenbruck, O., Weber, G. and Brockmann, E. (2014). The system GLONASS in April: What went wrong, *GPS World*, 24 June 2014. Available at: www.gpsworld.com/the-system-glonass-in-april-what-went-wrong/ (Accessed: 25 January 2026).
10. Saarinen, J. (2016). Satellite failure caused global GPS timing anomaly. *ITNews*, 28 January 2016. Available at: www.itnews.com.au/news/satellite-failure-caused-global-gps-timing-anomaly-414237 (Accessed: 25 January 2026).
11. OPSGROUP (2025). Worldwide GPS Dual Failure mystery solved. *OPSGROUP*. 28 May 2025. Available at: https://ops.group/blog/worldwide-gps-dual-failures (Accessed: 25 January 2026).
12. European Commission (EC) (2012). EGNOS Service Notice #5. 19 July 2012. Brussels: European Commission. Available at: https://egnos.gsc-europa.eu/documents/service-notice-5-egnos-service-unavailability-23-26-june-2012 (Accessed: 25 January 2026).
13. Chatre, E., Benedicto, J. (2019). 2019 – Galileo Programme Update, *Proceedings of ION GNSS+ 2019*, Miami, Florida, September 2019. Available at: https://doi.org/10.33012/2019.16900 (Accessed: 25 January 2026).
14. Federal Aviation Administration (FAA) (2019). *WAAS service advisories and NOTAMs relating to LPV service unavailability*. Washington DC: Federal Aviation Administration. Available at: www.faa.gov/air_traffic/flight_info/aeronav/safety_alerts/ (Accessed: 25 January 2026).
15. Nally, J. (2023). SouthPAN service outage following Inmarsat failure. *Spatial Source*, 19 April 2023. Available at: www.spatialsource.com.au/southpan-service-outage-following-inmarsat-failure/ (Accessed: 25 January 2026).
16. Inside GNSS (2013). FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS. *Inside GNSS*, 31 August 2013. Available at: https://insidegnss.com/fcc-fines-operator-of-gps-jammer-that-affected-newark-airport-gbas/ (Accessed: 25 January 2026).
17. Bockmann, M. (2019). Seized UK tanker likely spoofed by Iran. *Lloyd's List*, 16 August 2019. Available at: www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran (Accessed: 25 January 2026).
18. London Economics (2024). *GNSS disruption impacts at Denver and Dallas-Fort Worth airports*. London Economics, London, May 2024. Available at: https://rntfnd.org/wp-content/uploads/LE-RNTFND-Disruption-at-DEN-and-DFW-in-2022-FINAL29052024_PRINT.pdf (Accessed 25 August 2025).
19. Goward, D. (2019). NASA report: Passenger aircraft nearly crashes due GPS disruption, *GPS World*, 8 July 2019. Available at: www.gpsworld.com/nasa-report-passenger-aircraft-nearly-crashes-due-gps-disruption (Accessed: 25 January 2026).
20. Gowans, G. (2023). GPS jammer that brought disruption to Lyon Airport. *Trans.iNFO*, 17 July 2023. Available at: https://trans.info/en/gps-jammer-that-brought-disruption-to-lyon-airport-353510 (Accessed: 25 January 2026).
21. Bagirova., N. and Stolyarov., G. (2024). Russian air-defense system downed Azerbaijan plane, sources say. *Reuters*, 27 December 2024. Available at: www.reuters.com/world/asia-pacific/azerbaijan-airlines-flight-was-downed-by-russian-air-defence-system-four-sources-2024-12-26/ (Accessed: 25 January 2026).
22. Inside GNSS (2025). MSC Antonia grounding in the Red Sea attributed to suspected GPS spoofing. *Inside GNSS*, 15 May 2025. Available at: https://insidegnss.com/msc-antonia-grounding-in-the-red-sea-attributed-to-suspected-gps-spoofing/ (Accessed: 24 December 2025).
23. Chronos Technology (2014). *Sentinel Project – Report on GNSS Vulnerabilities*. Available at: https://chronos.uk/wordpress/wp-content/uploads/SENTINEL-Project-Report.pdf (Accessed: 25 January 2026).
24. C4ADS (2019). *Above us only stars "Exposing GPS Spoofing Russia and Syria"*. Available at https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf (Accessed: 25 January 2026).
25. OPSGROUP (2024). *Global GPS Interference Map and reporting archive*. Available at: https://ops.group/blog/worldwide-gps-dual-failures/ (Accessed 25 August 2025).
26. GPS Patron (2025). *Report on GNSS Interference in the Baltic Sea: Analysis Using a Terrestrial Monitoring System and Comparison with ADS-B Data*. Available at: https://gpspatron.com/gnss-interference-in-the-baltic-sea-a-collaborative-study-by-gpspatron-and-gdynia-maritime-university/ (Accessed: 25 January 2026).
27. Critical Infrastructure Security Centre (CISA) (2025). *Malicious insider risk*. Canberra: Department of Home Affairs. Available at: www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-malicious-insider-risk.pdf (Accessed: 25 January 2026).

28. NASA Office of Inspector General (2019). *Semiannual Report to Congress*, October 1, 2018 – March 31, 2019. Washington DC: National Aeronautics and Space Administration (NASA). Available at: www.oversight.gov/sites/default/files/documents/reports/2019-05/SAR0319.pdf (Accessed: 25 January 2026).

29. Lee, R.M., Assante, M.J. & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Institute*. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (Accessed: 25 January 2026).

30. Yang, D.I.-K. (2025). China's dual-use infrastructure in the Pacific. Coastwatchers 2.0, Institute for National Defense and Security Research. *Synopsis / SSANSE report*. Available at: www.canterbury.ac.nz/content/dam/uoc-main-site/documents/pdfs/Domingo,I_China%E2%80%99s_Dual-Use_Infrastructure_in_the_Pacific_final5.pdf (Accessed: 25 January 2026).

31. Parkinson, B.W. and Spilker, J.J. (eds.) (1996). *Global Positioning System: Theory and Applications, Volume I*. Washington, DC. American Institute of Aeronautics and Astronautics.

32. Kaplan, E.D. and Hegarty, C.J. (eds.) (2006). *Understanding GPS: Principles and Applications*. 2nd edition. Boston, MA: Artech House.

33. Department of Homeland Security (DHS) (2019). *Upcoming Global Positioning System Week Number Rollover Event*. Memorandum for U.S. owners and operators using GPS to obtain UTC time. Washington DC: National Cybersecurity and Communications Integration Center (NCCIC). Available at: www.cisa.gov/sites/default/files/documents/Memorandum_on_GPS_2019.pdf (Accessed: 25 January 2026).

34. Indian Defence Research Wing (2025). *India's NAVIC Satellite Constellation Faces crisis as Majority of Satellites become Defunct*. Available at: https://idrw.org/indias-navic-satellite-constellation-faces-crisis-as-majority-of-satellites-become-defunct/ (Accessed: 25 January 2026).

35. David, L. (2021). China anti-satellite test creates worrisome debris cloud circling Earth. *Space.com*, 18 November 2021. Available at: www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html (Accessed 25 January 2026).

36. BBC News (2019). *India shoots down satellite in space test*. 28 March 2019. Available at: www.bbc.com/news/world-asia-india-47729568 (Accessed: 25 January 2026).

37. Hoffmann, F. (2021) Russia conducts direct-ascent anti-satellite test. *International Institute for Strategic Studies*, 25 November 2021. Available at: www.iiss.org/online-analysis/online-analysis/2021/11/russia-conducts-direct-ascent-anti-satellite-test/ (Accessed: 25 January 2026).

38. Harrison, T., Johnson, K., Roberts, T.G., Way, T. & Young, M. (2020). *Space Threat Assessment 2020*. Center for Strategic and International Studies (CSIS), Washington, DC. Available at: https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf (Accessed: 25 January 2026).

39. GPS World (2013). The Halloween Storms: When Solar Events Spooked the Skies, *GPS World*, 30 October 2013. Available at: www.gpsworld.com/the-halloween-storms-when-solar-events-spooked-the-skies/ (Accessed: 25 January 2026).

40. Jacobsen, K.S. & Andalsvik, Y.L. (2016). Overview of the 2015 St. Patrick's Day storm and its consequences for RTK and PPP positioning in Norway. *Journal of Space Weather and Space Climate*, 6, A9. Available at:www.swsc-journal.org/articles/swsc/pdf/2016/01/swsc150065.pdf (Accessed: 25 January 2026).

41. Redmon, R.J., Seaton, D.B., Steenburgh, R., He, J. & Rodriguez, J.V. (2018). September2017's geoeffective space weather and impacts to Caribbean radiocommunications during hurricane response. *Space Weather*, 16. Available at: https://doi.org/10.1029/2018SW001897 (Accessed: 25 January 2026).

42. Elvidge, S. & Themens, D.R. (2025). The probability of the May 2024 geomagnetic superstorm. *Space Weather*, 23. Available at: https://doi.org/10.1029/2024SW004113 (Accessed: 25 January 2026).

43. Rajesh, P.K., Lin, C.H.C., Otsuka, Y., Yamamoto, M., Chen, S.P., Lin, C.Y., Matsuo, T., Nishioka, M., Perwitasari, S., Jin, H. & Choi, J.M. (2025). Causal links to persisting daytime equatorial plasma bubbles over Asia-Pacific region following the geomagnetic storm on 01 December 2023. *Scientific Reports*, 15, 21500. Available at: www.nature.com/articles/s41598-025-08791-9.pdf (Accessed: 25 January 2026).

44. Geoscience Australia (GA) (2023). *SouthPAN SBAS coverage and service performance overview*. Canberra: Geoscience Australia.

45. O'Neill, C. (2019a). Mental models: Part I – Rethinking the peace–war spectrum. *The Forge, Australian Defence Force*. 12 May 2019. Available at: https://theforge.defence.gov.au/article/mental-models-part-i-rethinking-peace-war-spectrum (Accessed: 25 January 2026).

46. O'Neill, C. (2019b). Mental models: Part II – Cooperation, competition and conflict. *The Forge, Australian Defence Force*. 18 May 2019. Available at: https://theforge.defence.gov.au/article/mental-models-part-ii-cooperation-competition-and-conflict (Accessed: 25 January 2026).

47. ISO (2018). *ISO 31000: Risk management – Guidelines*. International Organization for Standardization, Geneva.

48. Paladin Risk (2026). *Risk Tip 3: Developing a consequence matrix*. Available at: https://paladinrisk.com.au/risk-tip-3-developing-consequence-matrix/ (Accessed: 25 January 2026).

49. Proctor, A. (2025). Towards a Structural Framework for PNT Situational Awareness. Rethink PNT Paper, 19 May 2025. Available at: https://rethinkpnt.com/2025/05/19/pnt-situational-awareness-thoughts-on-a-structured-approach/ (Accessed: 25 January 2026).

50. Critchley-Marrows, J.J.R. & Verspieren, Q. (2025). Ensuring PNT resilience in a time of navigation uncertainty. *Space Policy*, vol. 72, article 101665. Available at: www.sciencedirect.com/science/article/pii/S0265964624000560 (Accessed: 25 January 2026).

51. United States Space Force (USSF) (2025). *Modernized GPS operating system closer to operational integration*. Colorado Springs, CO: United States Space Force. Available at: www.spaceforce.mil/News/Article-Display/Article/4242898/modernized-gps-operating-system-closer-to-operational-integration (Accessed: 25 January 2026).

52. Divis., D.A. (2023). New CHIMERA signal enhancement could spoof-proof GPS receivers. *Inside GNSS*, 3 June 2019. Available at: https://insidegnss.com/new-chimera-signal-enhancement-could-spoof-proof-gps-receivers/ (Accessed: 25 January 2026).

53. European Union Agency for the Space Programme (EUSPA) (2024). *Galileo Open Service Navigation Message Authentication (OSNMA)*. Prague: European Union Agency for the Space Programme. Available at: www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma (Accessed: 25 January 2026).

54. Zhilenko, S. (2025). GLONASS Status and Plans of Development. *Proceedings of the 19th Meeting of the International Committee on GNSS (ICG-19)*, 20 October 2025, Vienna.

55. Jun, L. (2024). Development of Beidou Navigation Satellite System. *Proceedings of 67th Session of the UN Committee on the Peaceful Uses of Outer Space*, Vienna, 17 June 2024. Available at: www.unoosa.org/documents/pdf/copuos/2024/Technical_Presentations/25/4_item_9_Development_of_BeiDou_Navigation_Satellite_System_LU_Jun_20240617CUPUOS-67.pdf (Accessed: 25 January 2026).

56. Air Force Research Laboratory (AFRL) (2025). *Navigation Technology Satellite-3*. Wright-Patterson Air Force Base, OH: Air Force Research Laboratory. Available at: https://afresearchlab.com/technology/nts-3 (Accessed: 25 January 2026).

57. NLA International (2025b). *Supporting the UK Public Sector in PNT Awareness, Research and Knowledge (SPARK). Part 2 – Satellite Based Augmentation Systems Report*. NLA International.

58. European Union Agency for the Space Programme (EUSPA) (2025). *GNSS and Secure SATCOM User Technology Report*. Issue 1. Prague: European Union Agency for the Space Programme. Available at www.euspa.europa.eu/sites/default/files/documents/GNSS_Secure_SATCOM_User_Tech_Report.pdf (Accessed 25 August 2025).

59. FrontierSI (2024). State of the Market Report, Low Earth Orbit Positioning Navigation and Timing – 2024 Edition, Available at https://frontiersi.com.au/wp-content/uploads/2025/01/FrontierSI-State-of-Market-Report-LEO-PNT-2024-Edition-v1.1.pdf (Accessed: 25 January 2026).

60. Kassas, Z., Neinavaie, M., Khalife, J., Khairallah, N., Haidar-Ahmad, J., Kozhaya, S. & Shadram, Z. (2024). Enter LEO on the GNSS stage: Navigation with Starlink satellites. *Inside GNSS*, 29 November 2021. Available at: https://insidegnss.com/enter-leo-on-the-gnss-stage-navigation-with-starlink-satellites/ (Accessed: 25 January 2026).

61. 3rd Generation Partnership Project (3GPP) (2024a). *About 3GPP*. Available at: www.3gpp.org/about-3gpp (Accessed: 25 January 2026).

62. European Commission (EC) (2024). *IRIS²: Europe's Secure Connectivity Programme*. Brussels: European Commission. Available at: https://defence-industry-space.ec.europa.eu/eu-space/iris2_en (Accessed: 25 January 2026).

63. Brown, A. & Koury, W. (2025) Deployment of a hybrid GEO/LEO solution as a Backup to GPS through PNT as a Service (PNTaaS). *Proceedings of the National Defense Industrial Association (NDIA) Emerging Technologies for Defense Conference and Exhibition*, 27 August 2025, Washington D.C. Available at: www.navsys.com/s/NDIA-ETI_Deployment-of-a-hybrid-GEO-LEO-solution-as-a-Backup-to-GPS.pdf (Accessed: 25 January 2026).

64. Brown, A., Reese, C. & Nguyen, D. (2025) Leveraging Commercial SATCOM as Signals of Opportunity through PNT as a Service (PNTaaS). *Proceedings of 2025 Joint Navigation Conference, Greater Cincinnati Area*, June 2025. Available at: www.navsys.com/s/NAVSYS-25-06-003-JNC-2025_-Signals-of-Opportunity-SoOp.pdf (Accessed: 25 January 2026).

65. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (2023b). *VHF Data Exchange System (VDES) Overview. Guideline G1117, Edition 3.0*. Paris: International Association of Marine Aids to Navigation and Lighthouse Authorities. Available at: www.iala.int/product/g1117/?download=true (Accessed: 25 January 2026).

66. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (2023a). *VDES and R-Mode Overview – IALA Guideline G1158, Edition 1*. Paris: International Association of Marine Aids to Navigation and Lighthouse Authorities. Available at: www.iala.int/product/g1158/?download=true (Accessed: 25 January 2026).

67. Australian Maritime Safety Authority (AMSA) (2023). *Navigation Services in Australia: Outlook to 2035*. Canberra: Australian Maritime Safety Authority. Available at: www.amsa.gov.au/sites/default/files/fn-navigation-services-in-australia-outlook-to-2035_0.pdf (Accessed: 25 January 2026).

68. Grant, A. & Goward, D (2022). 10 Answers about eLoran. *GPS World*, 11 April 2022. Available at: www.gpsworld.com/10-answers-about-eloran/ (Accessed: 25 January 2026).

69. Chronos Technology (2015). Delivering a national timescale using eLoran. Issue 1.0, 12 August 2015. Available at: https://chronos.uk/wordpress/wp-content/uploads/Delivering-a-National-Timescale-Using-eLoran-Ver1.1.pdf (Accessed: 25 January 2026).

70. UrsaNav (2016). eLoran points of light. Available at: http://ursanav.com/wp2024/wp-content/uploads/2024/11/eLoran-Points-of-Light-NOV2024-1.pdf (Accessed: 25 January 2026).

71. Inside GNSS (2017). South Korea developing an eLoran network to protect ships from cyber-attacks. *Inside GNSS*, 23 August 2017. Available at: https://insidegnss.com/south-korea-developing-an-eloran-network-to-protect-ships-from-cyber-attacks/ (Accessed: 25 January 2026).

72. Government Office for Science (2022). *Satellite navigation and timing: Resilient Position, Navigation and Timing – A Blackett Review.* London: Government Office for Science. Available at: https://assets.publishing.service.gov.uk/media/5a82c84ced915d74e34038ab/satellite-derived-time-and-position-blackett-review.pdf (Accessed: 25 January 2026).

73. Inside GNSS (2025). UK commits £155 million to eLoran, Timing and GNSS Monitoring in Major PNT Resilience Push. *Inside GNSS*. 19 November 2025. Available at: https://insidegnss.com/uk-commits-155-million-to-eloran-timing-and-gnss-monitoring-in-major-pnt-resilience-push/ (Accessed: 25 January 2026).

74. Yang, C., Li, S. & Hu, Z. (2023). Analysis of the Development Status of eLoran Time Service System in China. *Applied Sciences, 1*3, 12703. Available at: www.mdpi.com/2076-3417/13/23/12703 (Accessed: 25 January 2026).

75. Resilient Navigation and Timing Foundation (RNTF) (2023). Saudi Arabia upgrading to eLoran. Resilient Navigation and Timing Foundation. 9 June 2023. Available at: https://rntfnd.org/2023/06/09/saudi-arabia-upgrading-to-eloran/ (Accessed: 25 January 2026).

76. Bass, V., Efremov, P., Zarubin, S., Tsarev, V. & Choglokov, A. (2008). Present status and future developments of the Russian radionavigation system Chayka and joint Chayka/Loran-C radionavigation chains. *Proceedings of the International Loran Association Annual Meeting*. 28 October 2008, London, UK. Available at: https://loran.org/proceedings/Meeting2008/Papers/Tsarev_Reserve.pdf (Accessed: 25 January 2026).

77. Grundhöfer, L., Rizzi, F.G., Gewies, S., Hoppe, M., Bäckstedt, J., Dziewicki, M. & Galdo G. (2021). Positioning with medium frequency R-Mode. *Navigation*, 68(4). Available at: https://navi.ion.org/content/68/4/829 (Accessed: 25 January 2026).

78. Johnson, G.W., Swaszek, P.F., Dykstra, K. & Ordell, S. (2020). R-Mode Positioning System Demonstration. *Proceedings of ION GNSS+ 2020*, September 2020. Available at: www.ion.org/publications/abstract.cfm?articleID=17728 (Accessed: 25 January 2026).

79. Shyshkin, O.V., Konovets, V.I. & Koshevyy, V.M. (2024). AIS R-Mode Trilateration for GPS Positioning and Timing Insurance. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, 18(2). Available at: www.transnav.eu/files/AIS_RMode_Trilateration_for_GPS_Positioning_and_Timing_Insurance,1408.pdf (Accessed: 25 January 2026).

80. Bonenberg, L., Motella, B. & Fortuny-Guasch, J. (2023). Assessing Alternative Positioning, Navigation, and Timing Technologies for Potential Deployment in the EU. *Publications Office of the European Union*. Luxembourg, 2023. Available at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC132737/JRC132737_01.pdf (Accessed: 25 January 2026).

81. Gambale, N., Small, D., Barnes, J., Sainsbery, I., Gumbrell, C., Kanli, M. & Skeen, M. (2025). Locata: Time Flies… breakthrough timing over the air. *Inside GNSS*, 27 January 2025. Available at: https://insidegnss.com/locata-time-fliesbreakthrough-timing-over-the-air/ (Accessed: 25 January 2026).

82. Locata Corporation (2022). Locata DEFIS Demo Day presentations. *European Commission Directorate-General for Defence Industry and Space (DEFIS)*. Brussels, 18 May 2022. Available at: https://locata.squarespace.com/s/Locata-DEFIS-Demo-Day-Presentations-COMPLETE-9-May-2023.pdf (Accessed: 25 January 2026).

83. Mondal, T., Weller, R.D. and Matheny, S. (2021). Broadcast Positioning System Using ATSC 3.0. *Proceedings of the 2021 NAB Broadcast Engineering and Information Technology (BEIT) Conference, National Association of Broadcasters*, Washington, DC. Available at: www.nab.org/bps/Broadcast_Positioning_System_Using_ATSC30.pdf (Accessed: 25 January 2026).

84. Jeffs, E. (2025). *NextNav to Begin Operating World's First 5G-Powered PNT Network, Marking Major Step Toward Commercialization*, 11 December 2025. Available at: https://nextnav.com/begin-operating-worlds-first-5g-powered-pnt-network/ (Accessed: 25 January 2026).

85. 3rd Generation Partnership Project (3GPP) (2024b). TS 38.305 – NR; Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN, 3rd Generation Partnership Project. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3506 (Accessed: 25 January 2026).

86. International Telecommunication Union (ITU) (2019). *Recommendation ITU-R TF.1153-4: The operational use of two-way satellite time and frequency transfer (TWSTFT)*. Geneva: International Telecommunication Union. Available at: www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.1153-4-201508-I!!PDF-E.pdf (Accessed: 25 January 2026).

87. Blonski, D., Giorgi, G., Ibanez, D., Ávila Rodríguez, J.A. and Meurer, M. (2025). OpSTAR – The ESA Demonstrator of the Optical Future of PNT. *Proceedings of the 38th ION GNSS+ 2025*, September 2025. Available at: www.ion.org/publications/abstract.cfm?articleID=20437 (Accessed: 25 January 2026).

88. Kaur, N., Frank, F., Pottie, P-E. & Tuckey, P. (2017). Time transfer over a White Rabbit network. *First-TF General Assembly, Institut d'Optique d'Aquitaine*, June 2017. Available at: https://first-tf.com/wp-content/uploads/2017/06/FIRSTTF_AG2017_Doctorat_NamneetKaur.pdf (Accessed: 25 January 2026).

89. Range Commanders Council (2016). IRIG Serial Time Code Formats (IRIG Standard 200-16). *White Sands Missile Range, NM: Secretariat, Range Commanders Council*. Available at: www.irig106.org/docs/rcc/200-16_IRIG_Serial_Time_Code_Formats.pdf (Accessed: 25 January 2026).

90. D. Veitch, Ridoux, J. & Korada, S.B (2008). Robust Synchronization of Absolute and Difference Clocks Over Networks, in *IEEE/ACM Transactions on Networking*, 17(2). Available at: https://ieeexplore.ieee.org/document/4569868 (Accessed: 25 January 2026).

91. International Telecommunications Union (ITU) (2024). *Recommendation ITU-T G.8275.1, Precision time protocol telecom profile for phase/time synchronisation with full timing support from the network, Amendment 2*. Geneva: International Telecommunication Union. Available at: www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.8275.1-202408-I!Amd2!PDF-E&type=items (Accessed: 25 January 2026).

92. Institute of Electrical and Electronics Engineers (IEEE) (2020). *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, in IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008), 16 June 2020. Available at: https://ieeexplore.ieee.org/document/9120376 (Accessed: 25 January 2026).

93. European GNSS Agency (GSA) (2018). *Report on Time & Synchronisation User Needs and Requirements*. Issue 1.0, GSA-MKD-TS-UREQ-233690, 18 October 2018. Prague: European GNSS Agency. Available at: www.euspa.europa.eu/sites/default/files/documents/Report_on_User_Needs_and_Requirements_Timing_Synchronisation.pdf (Accessed: 25 January 2026).

94. UK Government (2023). *Government Policy Framework for Greater Position, Navigation and Timing (PNT) Resilience*, written statement, 18 October 2023. Available at: https://questions-statements.parliament.uk/written-statements/detail/2023-10-18/hcws1073 (Accessed: 27 December 2025).

95. National Institute of Standards and Technology (NIST) (2019). *Profile for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. NISTIR 8283*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8323r1.pdf (Accessed: 25 January 2026).

96. Cassel, R.S., Tobias, W.G. & Marlow, B.L. (2023). *Quantum vs. Classical Complementary PNT: Are quantum sensors the next big thing for PNT, or are they overhyped?* The MITRE Corporation, March 2023. Available at: www.mitre.org/sites/default/files/2024-06/PR-23-0577-Quantum-vs-Classical-Complementary-PNT.pdf (Accessed: 25 January 2026).

97. El-Sheimy, N. & Youssef, A. (2020). Inertial sensors technologies for navigation applications: state of the art and future trends. *Satellite Navigation 1*, 2. Available at: https://link.springer.com/article/10.1186/s43020-019-0001-5 (Accessed: 25 January 2026).

98. Vidal Bustamante, C.M. (2025). *Atomic Advantage: Accelerating U.S. Quantum Sensing for Next-Generation Positioning, Navigation, and Timing*. Washington, DC: Center for a New American Security (CNAS). Available at: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Quantum-Navigation-_TECH_May2025_FinalB.pdf (Accessed: 25 January 2026).

99. Li, H., Zaminpardaz, S., Kealy, A., Greentree, A.D., Rubinov, E., Gibson, B. & Choy, S. (2025). Quantum Sensors for Enhanced Positioning and Navigation: A Comprehensive Review. In press.

100. Lenz, J. & Edelstein, S. (2006). Magnetic sensors and their applications. *IEEE Sensors Journal*, 6(3). Available at https://ieeexplore.ieee.org/document/1634415 (Accessed: 25 January 2026).

101. AstraNav (2025). *Solutions*. Available at: www.astranav.com/solutions (Accessed: 25 January 2026).

102. iDvera (2025). *ALIS Trust Layer.* Available at: https://idvera.com/blog/alis-trust-layer.html (Accessed: 25 January 2026).

103. Muradoğlu, M., Johnsson, M.T., Wilson, N.M., Cohen, Y., Shin, D., Navickas, T., Pyragius, T., Thomas, D., Thompson, D., Moore, S.I., Rahman, M.T., Walker, A., Dutta, I., Bojanala, S., Berlocher, J., Hush, M.R., Anderson, R.P., Szigeti, S.S. & Biercuk, M.J. (2025). Quantum-assured magnetic navigation achieves positioning accuracy better than a strategic-grade INS in airborne and ground-based field trials. *Q-CTRL*, Sydney Australia. Available at: https://arxiv.org/abs/2504.08167 (Accessed: 25 January 2026).

104. Jones, M. (2017). Anti-jam technology: Demystifying the CRPA. *GPS World*, 12 April 2017. Available at: www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/ (Accessed: 25 January 2026).

105. Khalil, J. (2025). CRPAs for PNT removed from ITAR list. *GPS World*, 29 January 2025. Available at: www.gpsworld.com/crpas-for-pnt-removed-from-itar-list/ (Accessed: 25 January 2026).

106. Bisnath, S. (2023). The use and promise of artificial intelligence in GNSS PNT. *GPS World*. 23 May 2023. Available at: www.gpsworld.com/the-use-and-promise-of-artificial-intelligence-in-gnss-pnt (Accessed: 25 January 2026).

107. Siemuri, A., Selvan, K., Kuusniemi, H., Valisuo, P. & Elmusrati, M.E. (2022). A systematic review of machine learning techniques for GNSS use cases. *IEEE Transactions on Aerospace and Electronic Systems*, 20(20). Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9937069 (Accessed: 25 January 2026).

108. Northrop Grumman (2023). *Artificial intelligence helps protect troops in denied GPS environments*. Available at: www.northropgrumman.com/what-we-do/mission-solutions/artificial-intelligence-and-machine-learning/protects-troops-in-denied-gps-environments (Accessed: 25 January 2026).

109. European Space Agency (ESA) (2024). *Artificial intelligence making its way into PNT. NAVISP Programme*. Available at: https://navisp.esa.int/news/article/Artificial%20Intelligence%20making%20its%20way%20into%20PNT (Accessed: 25 January 2026).

110. Tern.AI (2025). *Tern.AI – AI-driven alternative positioning and navigation solutions*. Available at: www.tern.ai/ (Accessed: 25 January 2026).

111. Van Dyke, K. (2024). IDM Plans and Complementary PNT Update. GPS Advisory Board Meeting, December 2024. Available at: www.gps.gov/sites/default/files/2025-06/AdvisoryMeetings_Van-Dyke_Dec2024.pdf (Accessed: 25 January 2026).

112. UK Government (2023). *Space-based PNT: Technical concepts*. Available at: www.gov.uk/government/publications/space-based-pnt-technical-concepts/space-based-pnt-technical-concepts (Accessed: 25 January 2026).

113. European Commission (2023). *European Radio Navigation Plan (ERNP)*. Luxembourg: Publications Office of the European Union. Available at: https://joint-research-centre.ec.europa.eu/document/download/02662742-1c5f-4ecf-9feb-6d808d8fc226_en?filename=ERNP-2023_EN_101a%201.pdf (Accessed: 25 January 2026).

114. Khalil, J. (2024). Australia and India advance resilient PNT. *GPS World*. 9 December 2024. Available at: www.gpsworld.com/australia-and-india-advance-resilient-pnt/ (Accessed: 25 January 2026).

115. Australian Government Department of Defence (2025). *Defence signs agreement for innovative sovereign space project*, media release. 14 July 2025. Available at: www.defence.gov.au/news-events/releases/2025-07-14/defence-signs-agreement-innovative-sovereign-space-project (Accessed: 25 January 2026).

116. AMSA (2020). Australia's differential global positioning system. 1 July 2020. Available at: www.amsa.gov.au/safety-navigation/navigation-systems/australias-differential-global-positioning-system (Accessed: 25 January 2026).

117. Safety4Sea (2019). AMSA to discontinue its Differential Global Positioning System service. 14 November 2019. Available at: https://safety4sea.com/amsa-to-discontinue-its-differential-global-positioning-system-service/ (Accessed: 25 January 2026).

118. Kawecki, J., Brewer, J., Cao, J., 746th Test Squadron & Baldwin, J. (2016). Can't deny the truth: Air Force upgrades to a better field reference system for testing GPS denial, *GPS World*, August 2016. Available at: www.gpsworld.com/air-force-upgrades-to-better-field-reference-system-for-testing-gps-denial/ (Accessed: 25 January 2026).

119. AARNet (2025). *AARNet Network Overview*. Available at: www.aarnet.edu.au/ (Accessed: 25 January 2026).

120. US Department of Transportation (2021). *FY2021 NDAA Section 1606: Report to Congress on the National Positioning, Navigation, and Timing Architecture*. Washington, DC: USDOT. Available at: www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_January%202021.pdf (Accessed: 25 January 2026).

121. Hansen, A., Mackey, S., Wassaf, H., Shah, V., Wallischeck, E., Scarpone, C., Barzach, M. & Baskerville, E. (2021). Complementary PNT and GPS Backup Technologies Demonstration Report. DOT-VNTSC-20-07, U.S. Department of Transportation, January 2021. Available at: www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_Combinedv2_January%202021.pdf (Accessed: 25 January 2026).

122. Shaw, G., Williams, P., Fairbanks, M. & Airey, T. (2020). MarRINav – Maritime Resilience and Integrity in Navigation, Final Report v1.0., NLA International Ltd., 25 March 2020. Available at: https://marrinav.com/wp-content/uploads/2020/04/20-03-25-Final-Report-MarRINav-v1.0.pdf (Accessed: 25 January 2026).

FRONTIER SI

We know where.

frontiersi.com.au