FRONTIER SI

ASSESSING PNT DISRUPTIONS AND THEIR IMPACTS ON DEFENCE

SCENARIO PLANNING AND RISK ANALYSIS

January 2025

FRONTIER SI

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 continues 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 Department of Defence Strategic Policy Grants Program.

Primary authors:

- Jia Lee (FrontierSI)
- Eldar Rubinov (FrontierSI)

FrontierSI would like to acknowledge expert input from:

- Joshua Critchley-Marrows (Independent)
- Owen Cooper (ANU National Security College)

Valuable feedback was received from personnel from:

- Department of Defence
- Department of Home Affairs
- Geoscience Australia
- Australian Maritime Safety Authority
- James Leversha, Graeme Kernich (FrontierSI)

CREATIVE COMMONS LICENSE

Citation

FrontierSI (2025), Assessing PNT Disruptions and Their Impacts on Defence: Scenario Planning and Risk Analysis, available at frontiersi.com.au.

CONTENTS

ABBREVIATIONS

ADF	Australian Defence Force
C5ISR	Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance
eLORAN	Enhanced Long Range Navigation
EM/ EMS	Electromagnetic / Electromagnetic Spectrum
GEO	Geostationary (satellite)
GPS	Global Positioning System
GNSS	Global Navigational Satellite Systems
HF	High Frequency
LEO	Low Earth Orbit
PNT	Positioning, Navigation and Timing
RAN	Royal Australian Navy
RF	Radio Frequency
SBAS	Satellite Based Augmentation System
SouthPAN	Southern Positioning Augmentation Network
USSF	United States Space Force

EXECUTIVE SUMMARY

Context

Positioning, navigation and timing (PNT) information is vital to all warfighting platforms, mission-critical operations, and supporting systems within the Australian Defence Force (ADF). In an increasingly complex geostrategic and warfighting environment, access to assured and resilient PNT is a key requirement for the Department of Defence's (Defence) capabilities to achieve the strategic posture described in the 2024 National Defence Strategy.

There are no open-source examples of scenario planning or tabletop exercises in Australia specifically addressing the disruption of Global Navigation Satellite Systems (GNSS), particularly with a Defence focus. In 2024, the Australian Government conducted exercises examining the effects of catastrophic disruptions to Australian critical infrastructure. However, these exercises provided only limited coverage on disruptions to PNT and impacts to critical infrastructure. Details of classified exercises or wargames are not available to the public.

To address this gap, FrontierSI designed a Defence-focused scenario exercise to examine situations where Australia's ability to deter is compromised, with special consideration of situations when PNT is degraded or denied. The resulting exercise featured two scenarios, each comprising three injects (events to advance the scenarios) designed to evaluate responses to escalating disruptions of the Global Positioning System (GPS), within the context of intensifying conflict. The exercise brought together 20 government representatives from Defence, Geoscience Australia, Department of Home Affairs, and the Australian Maritime Safety Authority to collaboratively explore these scenarios. The objectives of the workshop were:

- To explore responses of different personnel across Defence and key civilian government agencies at the OFFICIAL level to domain-specific and/or national-level disruptions of PNT.
- To investigate high-level interdependencies and impacts to PNT in denied, degraded or contested environments, treating fundamental components of domains, platforms, and supporting critical infrastructure.

Results

Scenario 1 Inject 1 involves a space weather event and opportunistic cyber hack impacting GPS signal integrity. Signals remain available but are degraded for 24-48 hours. The compounded effects of the space weather event and compromised GPS ground infrastructure is found to potentially lead to moderate implications in the land, air, space and cyber domains, while the maritime domain remains relatively unaffected at this stage. Overall, Defence is anticipated to demonstrate moderate resilience to this threat scenario. However, this categorisation is qualitative, relative, and optimistic. It should not be represented as a false reassurance of Defence's PNT capabilities, as there is a lack of understanding of cascading impacts beyond the individual domains at the enterprise level.

Scenario 1 Inject 2 explores Australia's response to a lack of PNT sovereignty and command and control, during which time a short-term 24-hour GPS outage is enforced out of necessity. By this stage, all Defence domains would be heavily impacted including maritime. Concerningly, several of Defence's major systems and networks would be unserviceable, including weapons systems, shared allied systems, and the Defence IT networks on which its logistics and health planning capabilities are hosted. Loss of many critical services is attributed to a loss of time synchronisation, which then becomes a pressing Defence and national issue with no viable, scalable alternative. Defence's resilience to a blanket GPS outage for 24 hours would be low.

Scenario 1 Inject 3 presents a non-kinetic attack in-orbit, contributing to a prolonged blanket GPS outage. Critical infrastructure services on which Defence relies on would be severely impaired, including the national grid, fuel supply, and logistics. By this stage, the national posture may shift from crisis to conflict, exacerbated by a loss of social cohesion. Alarmingly, Australia lacks a clear central authority for the restoration of PNT services in Australia. Defence's resilience to a sustained GPS outage would be low, characterised by severe consequences to critical infrastructure, ADF operations across all domains, C5ISR capabilities, and public safety.

Scenario 2 Inject 1 involves a joint maritime exercise in the South China Sea disrupted by GPS jamming, possibly linked to another nation's military exercise nearby to project power. Although the direct impact across the fleet appears limited, the quality of the exercise may be diminished. Australia has not encountered the high levels of jamming observed in other conflict zones. However, the threat remains credible, and the likelihood of grey zone activities in the region is significant. Without proactive measures to address this threat, Defence's PNT resilience would remain low.

Scenario 2 Inject 2 redirects the fleet to perform a search and rescue mission in the open seas amidst persistent GPS jamming by an adversary. While the likelihood of the threat is high, the overall impact to ADF operations, affected domains, and public perception and safety is qualitatively assessed as moderate, with some civilian collateral effects anticipated. The consequences of the threat are partly mitigated by the proficiency of naval personnel in traditional and alternative methods for navigation. However, the same reliable backups are either unavailable or not applicable in other domains, such as air operations. Additionally, the loss of GPS-enabled time synchronisation cannot be readily replaced by traditional methods. As with the previous inject, if Defence does not take steps to address its primary vulnerability – overreliance on GPS – its PNT resilience will remain low.

Scenario 2 Inject 3 involves Australia's role in a maritime contingency to support allies amidst escalating geopolitical tensions, disrupted by targeted, long-range GPS spoofing. The disruption is expected to impair C5ISR coordination with allies, compromise fleet security and domain awareness, and jeopardise mission objectives. Defence's PNT resilience is assessed as low, highlighting critical vulnerabilities to operate effectively under such conditions.

Shifting towards a resilient PNT posture

Based on a qualitative Threat-Consequence matrix and mapping of summarised responses, Defence's overall PNT resilience is found to be low. In Scenario 1, the threats to PNT – such as a forced reset of the GPS service compounded by an in-orbit non-kinetic attack – are considered highly unlikely with little precedent. However, the corresponding consequences are assessed as major to severe, primarily due to the limited preparedness of Defence, and Australia more broadly, to mitigate the impacts. This lack of readiness is partly attributed to risks associated with non-sovereign PNT assets and services, which Defence relies on but fall outside of Australia's immediate control. While Defence may have limited ability to reduce the likelihood of such threats, it can take proactive measures to shift from a "Low Resilience" posture towards "Moderate Resilience".

In Scenario 2, the threats – such as GPS jamming and spoofing in a maritime environment – are assessed as highly likely and have precedent. The immediate consequences are relatively moderate, reflecting Defence's naval capability to manage their response in contained situations. However, challenges are expected to arise in more complex scenarios. These include: i) mission-critical operations involve coordination between maritime, land and air domains; ii) the need for weapons systems readiness to maintain domain awareness and security; and iii) scenarios involving civilian collateral. Given the significance and frequency of GPS spoofing and jamming globally, Defence's overall PNT resilience in this scenario remains low. To shift Defence's resilience posture towards "Moderate Resilience", Defence must focus on both reducing the threat likelihood and mitigating the consequences.

The recommendations below need to be in place for Defence resilience, though not all initiatives need to be led by Defence. Note that these recommendations are intended to stimulate discussion. Any further considerations of prioritisation, progression, and investment in recommendations should be supported by additional validation beyond the scope of this report.

- **Recommendation 1:** Conduct a comprehensive PNT audit, based on cyber security risk management frameworks, to evaluate and characterise Defence's PNT resilience profile at the enterprise level.
- **Recommendation 2:** Designate a national backup time reference or network clock to enable both Defence and critical infrastructure systems to synchronise and connect to in a prioritised manner.
- **Recommendation 3:** Develop a robust national capability for GPS signal integrity monitoring and assurance, to identify, detect and respond to the loss of integrity of GPS signals.
- **Recommendation 4:** Develop a multi-source, multi-layered PNT architecture and capability to address the vulnerabilities of Defence reliance on GPS for its PNT needs.
- **Recommendation 5:** Undertake scenario planning, testing and training exercises across all domains, in environments where GPS is actively disabled, to identify, respond to, and mitigate vulnerable systems.
- **Recommendation 6:** Elevate discussions on spoofing threats and anti-spoofing capabilities within the Defence and national security agendas, ensuring comprehensive strategies are developed to address PNT risk management as critical components of cyber and electronic warfare.
- **Recommendation 7:** Expand and standardise training in traditional and alternative PNT techniques as an effective stop-gap measure, ensuring that personnel across multiple domains are Trained and Equipped to navigate and communicate in EMS-contested environments.
- **Recommendation 8:** Establish a designated centralised authority, such as a National PNT Office, to coordinate PNT initiatives across relevant government agencies, including Defence, create a cohesive national agenda aimed at enhancing PNT resilience.

1 INTRODUCTION

1.1 Background

Positioning, navigation and timing (PNT) information is vital to all warfighting platforms, mission-critical operations, and supporting systems within the Australian Defence Force (ADF). In an increasingly complex geostrategic and warfighting environment, access to assured and resilient PNT is a key requirement for Defence's capabilities to achieve the strategic posture described in the 2024 National Defence Strategy.[1]

PNT provides critical elements in defence operations as it enables precision, coordination, and situational awareness, which are essential for mission success. Accurate positioning allows forces to know their exact location, whether on land, sea, or air, facilitating tactical manoeuvres and avoiding friendly fire. Navigation ensures the ability to move through complex terrains and environments, maintain formation, and reach objectives effectively. Timing is crucial for synchronising operations, coordinating strikes, and efficiently targeting moments for action.

Together, resilient PNT capabilities enhance decision-making, reduce risks, and provide a strategic advantage in dynamic and hostile environments. In modern defence systems, PNT underpins technologies like guided weaponry, reconnaissance systems, and battlefield communication, underscoring its indispensability in ensuring operational effectiveness.

PNT services are not just used on the battlefield, they are foundational for all domains in critical civil infrastructure, including power grids, communication networks, and financial systems, where degradation can undermine the ability for Defence to operate effectively in Australia or at distance.

Key factors that challenge Defence's PNT resilience include:

- Defence's reliance on the US Global Positioning System (GPS), including constraints on accessing multi-GNSS sources due to stringent interoperability requirements.
- Defence's reliance on civilian and national critical infrastructure, which also depend on GPS for their navigation and time synchronisation requirements.
- GPS and overall Global Navigation Satellite Systems (GNSS) vulnerabilities arising from various threats.
- Lack of a Defence and/or national PNT strategy to guide development, implementation, and scaling of resilient PNT technologies, as well as a management action plan to coordinate and lead when GPS or GNSS is severely degraded or denied.

There is a lack of public discourse regarding PNT policy in Australia. A limited list of relevant literature is presented in the Appendix. This paper reports on a Defence-focused workshop that explored a set of scenarios when Australia's ability to deter is at risk, with special consideration of situations when PNT is degraded or denied.

1.2 Workshop rationale

The *PNT Disruption and Impacts on Defence* workshop was conducted by FrontierSI, supported by the Australian National University National Security College on 8 November 2024. The workshop was conducted at the OFFICIAL level and included participants from across multiple divisions and agencies of the Department of Defence, Department of Home Affairs, Geoscience Australia, and the Australian Maritime Safety Authority.

The workshop was sponsored by Defence as part of FrontierSI's Armouring the Clock project, under the Strategic Policy Grants Program.

The workshop objectives included the following:

- To explore responses of different personnel across Defence and key civilian government agencies to domain-specific and/or national-level disruptions of PNT.
- To investigate high-level interdependencies and impact to PNT in denied, degraded or contested environments, treating fundamental components of domains, platforms, and supporting critical infrastructure.
- To highlight gaps in enablers (such as policies, technology, data accessibility, information sharing, standards) that would enable Defence and other key stakeholders to respond effectively to the scenarios.
- To evaluate shortfalls in Australian Defence PNT capabilities and how this might translate to policy recommendations.
- To stimulate awareness across government portfolios on understanding and pre-empting scenarios on which critical PNT services are at risk, and the implications this may have on domain operations and situational awareness.

[1] https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program

2 SCENARIO DEVELOPMENT AND RATIONALE

2.1 Conceptualisation

There are no open-source examples of scenario planning or tabletop exercises for GNSS disruption in Australia, and certainly none that are Defence-focused. The Australian Government conducted several exercises in 2024 exploring the impacts of catastrophic disruptions to Australian critical infrastructure, including a national convention hosted by the Critical Infrastructure Advisory Council, space weather impacts hosted by the National Emergency Management Authority (Exercise Aurora[2]), and hypothetical wargames at space conferences. These exercises had limited coverage on disruptions to PNT and impacts to critical infrastructure, and neither have any post-exercise reports been made publicly available at this stage.

International trials and exercises do exist, but are geared towards detecting and identifying GNSS disruption, testing hardened receivers or emerging technologies, and jamming and spoofing exercises. Such examples include:

- The Harmonious Rook project, which tests commercial technologies to detect GNSS disruptions, and to identify and attribute GNSS threats through military exercises.[3]
- PNTAX, an annual PNT Assessment Experiment, to test and evaluate the effectiveness and interoperability of new technologies with military capabilities.[4]
- Jammertest, an annual open and staged spoofing and jamming event to test the resilience of GNSS and non-GNSS based systems.[5]

A gap exists for public discourse in Australia on disruptions to PNT and its flow-on effects across Defence domains and critical infrastructure. To examine Australia's preparedness for PNT outage events, FrontierSI designed a scenario planning exercise that brings in physical, natural, cyber, and supply chain threats to PNT. The scenarios were based around the following concepts:

- Events or trends that are recent or have precedence.
- Events that have not yet occurred but have a potential likelihood based on literature review.
- Known advancements in PNT technologies.
- Geopolitical tensions in the Indo-Pacific region, and Australia's foreign affairs policy.

In total, two scenarios were developed, unfolded through three exercise injects each, i.e. events introduced into the exercise that advance the scenario. Each inject was designed to assess responses to increasing severity of a GNSS and GPS disruption or denial within the context of growing geopolitical conflict. Table 1 provides information and rationale for the scenarios and injects.

[2] www.nema.gov.au/about-us/media-centre/exercise-aurora-preparing-australia-extreme-weather
[3] Inside GNSS, 2022. Upcoming Military Exercises to Focus on Detecting GNSS Disruption, https://insidegnss.com/upcoming-military-exercises-to-focus-on-detecting-gnss-disruption
[4] Winkler, 2023. Army conducts fifth annual Positioning, Navigation and Timing Assessment Experiment, www.army.mil/article/270791/army_conducts_fifth_annual_positioning_navigation_and_timing_assessment_experiment
[5] Jammertest, https://jammertest.no/jammertest

Table 1: Rationale for scenario and inject elements.

Scenario 1	Inject elements	Rationale for selection
Background	Space weather event	Impacts systems with safety specifications of 1-20 m. Errors become more adverse over time. Depending on quality, some common receivers may experience even worse performance.
Inject 1	Malicious attack on GPS master control station	To explore responses when the cause of GPS disruption has evolved from a natural hazard source, to now being a cyber-based threat.
Inject 2	GPS reset	To assess responses and actions due to a short term, blanket outage of GPS. To explore Defence's backup plans and if there was awareness to sovereign technologies for a situation lasting several hours.
Inject 3	EM charge pulse	To assess responses and actions due to an: i) extended outage of GPS; and ii) a situation that moves past grey zone towards conflict.

Scenario 2	Inject elements	Rationale for selection
Background	Live missile firing exercise in low-level jamming environment	To assess responses and actions in a situation when GPS navigation is not available for precision-guided missiles due to the impact of localised jamming from a non-military source.
Inject 1	Jamming due to another nation's military exercise	Introduces sophisticated, high-level, regional jamming from a military actor. The inject aims to examine processes and technologies for assured PNT.
Inject 2	Naval accident involving an allied survey ship and a merchant vessel	Involves another allied nation that also depends on GPS, given the UK has restricted access to Galileo since Brexit. Additionally, the elements provide a premise for another nation's unfriendly presence in the area as well as highlighting their asymmetric technological advantage over Australia.
Inject 3	Separate spoofing incident	Given jamming has different technical and political implications from spoofing, to explore what Defence considers as alternative technologies, including those with anti-spoof characteristics.

2.2 Scenarios and Injects

This section provides detailed information on each scenario and inject in Table 2 and Table 3.

Table 2. Scenario 1 details.

Scenario 1	
Background	• It is early 2025. • The Bureau of Meteorology (BoM) reports on a Coronal Mass Ejections event associated with the recent solar maximum. Extreme ionospheric activity will occur worldwide and will persist for approximately 24-48 hours. • The US Space Force (USSF) reports degraded GPS satellite signals, and Geoscience Australia advises that (SBAS) signals from the civilian SouthPAN service, which augments GPS signals for safety-of-life aviation systems, are also degraded. The EU, Russia and China also report minor degradations to their GNSS constellation signals. Media channels report that both military and civilian users worldwide have reported increased positioning noise, up to 20 m for some common receiver products. • Australia's power supplies are also affected, and the Trusted Information Sharing Network (TISN) has advised that several power grid stations in NSW are experiencing disruptions to normal operations. Defence Estate has reported that several Defence bases in NSW and QLD are using backup emergency power supplies. Early investigations from energy companies indicate the disruption is being caused by time synchronisation errors, related to GNSS signal degradation.
Inject 1	• The BoM has advised Defence that solar activity is reducing. However, users of GPS are still experiencing positioning issues. • Meanwhile, the USSF reports it has detected an intrusion at the GPS Master Control Station in Colorado USA. Attackers appear to have gained access remotely and manipulated the navigation message code of the GPS signal, exploiting a system configuration vulnerability at the Master Control Station. • USSF investigations discover that slightly erroneous ephemeris and clock parameters are being transmitted to GPS satellites via the uplink station. As a result, GPS satellites have been transmitting incorrect navigation messages, resulting in further positioning discrepancies. These errors have been incorrectly attributed to the effects of space weather. • The USSF is assessing several options for correction and will advise shortly.
Inject 2	• To correct the navigation message anomaly, the USSF has informed us that they must perform a GPS system reset. GPS services will be out of operation for 18-24 hours while the reset is completed. • The federal government has requested an urgent briefing on the situation, including affected capabilities and risks, and options for mitigation until the integrity of GPS can be guaranteed. • We have been tasked with ensuring that alternative and backup PNT means are available and accessible to critical Defence systems and can be deployed as soon as possible.
Inject 3	• The USSF informs us that an in-orbit electromagnetic pulse, ejected at approximately 20,000 km altitude, has disrupted the GPS satellite reset process. • Several GPS satellites have been compromised due to a temporary seizure of electronics, but they are not permanently damaged. • USSF expects GPS services to be unavailable for several days. • The government has requested an emergency update on the situation.

Table 3. Scenario 2 details.

Scenario 2	
Background	• It is early 2025. • Over the past few months, Defence is aware that indiscriminate GPS jamming has been occurring in the South China Sea, impacting activities from shipping to aviation. While the most recent jamming sources have not yet been confirmed, previous instances have been attributed mostly to localised jamming from piracy operations. • The ADF has agreed to conduct a joint live missile firing exercise with allied forces (Nation A), in waters west of Luzon. Just before exercise begins, a nation with divergent interests (Nation B) announces it will undertake its own military exercise in waters adjacent to Australia's planned exercise zone. • Australia and its Nation A agree to continue with the exercise.
Inject 1	• As Royal Australian Navy (RAN) vessels transit to the exercise area, they receive reports that port authorities are experiencing increasing disruption to their vessel traffic monitoring systems, which rely directly on GPS PNT information, broadcast by AIS signals. • The exercise begins amid high levels of jamming, impacting military vessels and aircraft. The jammers are directly impacting synchronisation across the RAN naval ships' integrated bridge system. Signal analysis indicates the jamming is being caused by Nation B naval vessels in the adjacent exercise area. • Given this heightened situation, the Armed Forces of Nation A seek Australia's views on which parts of the exercise, if any, should be cancelled or modified. The exercise is scheduled to include formation sailing, helicopter cross-deck exercises, replenishment-at-sea, anti-surface warfare drills, and live-firing of anti-ship missiles.
Inject 2	• As RAN vessels prepare to depart, they receive reports of a naval accident – one a merchant vessel registered to Nation B, the other a British survey ship – north of the contested Spratly Islands in the South China Sea. The RAN and Nation A military aircraft and naval vessels respond to the distress calls. • Nearing the accident site, the vessels observe several Nation B military and Coast Guard vessels. • RAN units continue to experience GPS jamming, including discrepancies between GNSS-based e-Navigation and secondary sensors, as well as obtaining system error messages regarding GPS. The Armed Forces of Nation A is reluctant to use aircraft for the search while GPS is not available. • Nation B issues its first statement regarding the accident, claiming that the British-flagged vessel caused the accident by a navigation error, and that its merchant vessel was using a 'proven, reliable' navigation system and not the 'increasingly unreliable' US-based GPS system.
Inject 3	• As the search and rescue operation concludes, US-China relationships are escalating over a situation in Taiwan. There is potential for Australia to be involved in a contingent supporting Taiwan at short notice. As a result, the RAN vessels have been ordered to head north towards Taiwan. • As the contingent approaches Taiwan open waters, one of the RAN ships' navigation systems shows the ship doing 50 knot speeds over ground. The contingent attributes this error to long range GPS spoofing. Not all vessels have reported this error. • The Defence Minister requests an urgent briefing on the situation, including affected capabilities and risks, and options for mitigation.

3 SCENARIO EXERCISE OUTCOMES AND RISK ANALYSIS

3.1 Analysis methodology

Participants collaborated in groups to identify key implications, discuss priorities, and explore potential response options (e.g. summary of responses in Table 8). Following the workshop, consequence maps were developed for each inject to visually summarise key vulnerabilities in the land, maritime, air, space and cyber domains (e.g. Figure 1). Additionally, risk matrices were developed to represent the risks (Threat Likelihood) and impacts (Consequence) presented by these injects (e.g. Table 9).

Threat Likelihood

FrontierSI's approach to developing the Risk matrices is qualitative and comparative. The analysis involves firstly, assessing the likelihood of occurrence of a threat, regardless of the type of threat or hazard vector to PNT (i.e. natural or physical, personnel, supply chain, cyber and information, as defined by the Cyber and Infrastructure Security Centre[6]).

We adapted a methodology for threat assessment from the Risk Management for US Department of Defense (DoD) Security Programs.[7] FrontierSI developed tailored guidance for assigning a Threat Likelihood rating (Table 4), informed by key themes identified during the workshop. Each inject from Scenarios 1 and 2 was assigned a Threat Likelihood rating with a corresponding score (1-5). This scoring system allows for a normalised analysis of both Threat and Consequence (see Section 3.4). The adapted approach for this project permits:

- Evaluation of the frequency of the threat, adversarial intent and capability, and precedence.
- Inclusion of natural threats to PNT, such as space weather, that may not typically be addressed in broader DoD security programs but are critical for PNT resilience.

Consequence

Secondly, FrontierSI adapted and customised an approach by Paladin[8] to categorise the consequences of risk across several critical factors. This method allows for a more structured analysis of each inject's impact, informed by key themes identified during the workshop.

FrontierSI developed tailored guidance for assigning a Consequence rating for each critical factor. Each inject was rated across critical factors with a corresponding score (1-5), then a non-weighted average applied to attain an overall Consequence score. The critical factors selected are:

Table 4. FrontierSI guidance for assigning a rating for a PNT Threat Likelihood.

Threat (Score)	Likelihood Description
Highly Likely (5)	Australian critical minerals provenance and traceability framework developed.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.

- Critical infrastructure and ADF operations (Table 5)
  - Ability to communicate and coordinate
  - Functionality of enterprise* operations and social systems
  - Functionality of governance and decision-making mechanisms at the national and/or enterprise* level
- Defence situational awareness (Table 6)
  - Extent of loss of C5ISR and situational awareness
  - Domains impacted
  - Whether the threat and/or impacts of the threat can be contained
  - Where mission objectives can be carried
- Public perception and safety (Table 7)
  - Loss of public confidence and social cohesion
  - Seriousness of casualties
  - Requirement for Defence to maintain civil unrest

** "Enterprise" may refer broadly to an organisation such as Defence or a government agency.*

[6] www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf
[7] www.cdse.edu/Portals/124/Documents/jobaids/general/GS102-JobAid.pdf
[8] https://paladinrisk.com.au/risk-tip-3-developing-consequence-matrix

Table 5. FrontierSI guidance for selecting a Consequence rating for impacts to critical infrastructure and ADF operations.

Consequence (Score)	Critical infrastructure and ADF operations
Severe (5)	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.
Major (4)	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.
Moderate (3)	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.
Minor (2)	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.
Insignificant (1)	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.

Table 6. FrontierSI guidance for selecting a Consequence rating for impacts to Defence situational awareness.

Consequence (Score)	Defence situational awareness
Severe (5)	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.
Major (4)	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.
Moderate (3)	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.
Minor (2)	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.
Insignificant (1)	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.

Table 7. FrontierSI guidance for selecting a Consequence rating for impacts to public perception and safety.

Consequence (Score)	Public perception and safety
Severe (5)	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Major (4)	Medium-term sense of insecurity amongst the public. Significant loss of confidence in government to manage and contain the threat. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Moderate (3)	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Minor (2)	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Insignificant (1)	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.2 Responses to Scenario 1

3.2.1 Scenario 1 Inject 1

Scenario 1 Inject 1 involves a space weather event and opportunistic cyber hack impacting GPS signal. Signals are degraded for 24-48 hours, but there is no blanket signal outage. Table 8 highlights participant responses to the inject, Figure 1 summarises the responses in a consequence map across Defence domains, and Table 9 analyses impacts in a risk matrix.

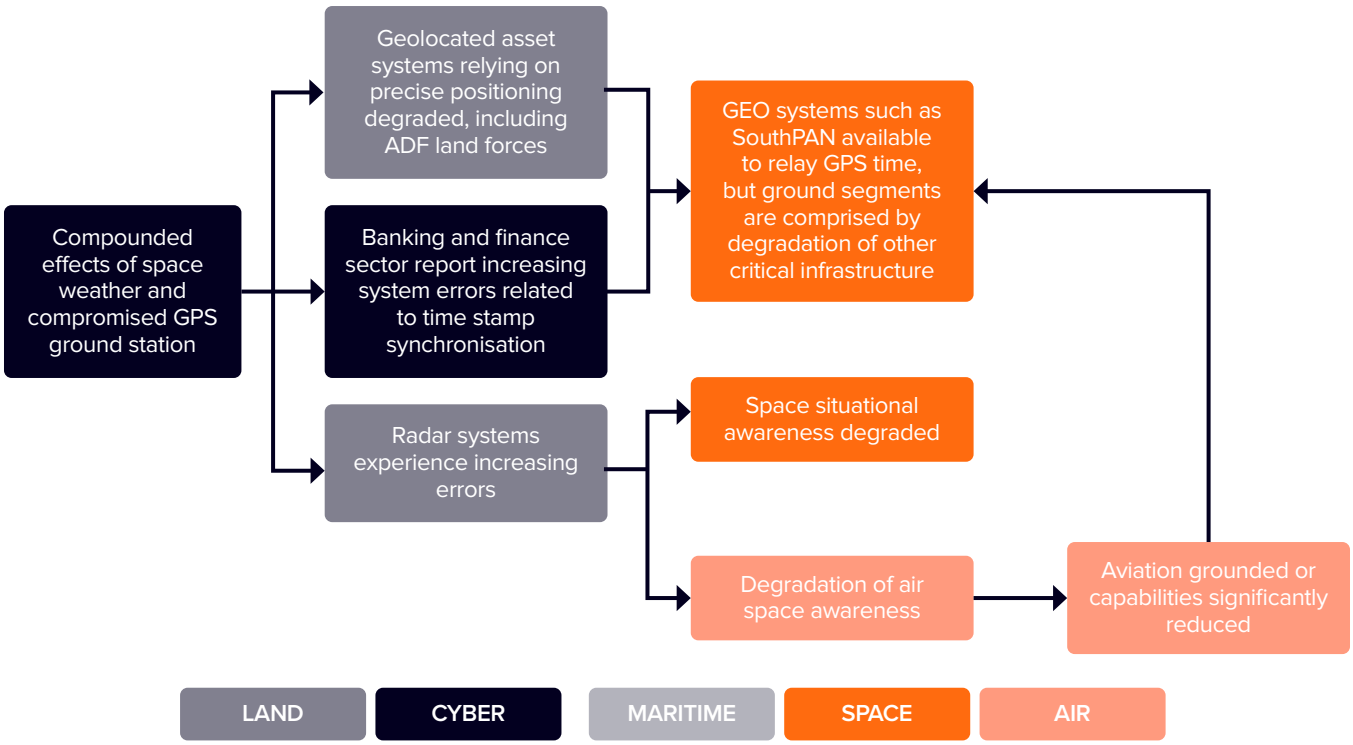
Table 8. Responses to Scenario 1 Inject 1.

Systems and services impacted
• Any operations where signals do not undergo corrections (example via a ground station or SBAS) will encounter some degradation. • Landing systems for aircraft and air traffic management. • At this stage impacts on maritime navigation are unlikely to be significant. • Services using time stamping, such as banking and finance, mobile phone towers, remote medical services. • Radar systems will experience increased errors. • Geolocated assets relying on precise positioning, including ADF location data. • Precision navigation and timing effects may be compounded by power-related issues.
Response and priorities
• Priorities are safety of life, safety of equipment, and security. • Triage and identify what systems and/or sectors have been affected.
Alternative systems or technologies
• Ground stations and SBAS can help correct for inaccuracies in positioning • Inertial navigation • Vision-based navigation
Issues with alternatives
• Alternative systems may not integrate with existing systems and need to be configured for interoperability in the first instance. • It is understood that Defence has risk mitigation plans including the prioritisation of activities and graceful degradation of systems. However, certain shared military systems reportedly lack the capability or permission to switch over from GPS to other GNSS. • Civilian infrastructure, such as Geoscience Australia's processing pipeline for SBAS signals, would be impacted by power outages. • SBAS and other civilian infrastructure and systems are not military-hardened and may lose the ability the keep monitoring SBAS signal integrity. • It is unclear what policies are available for GPS primary systems to switch over to other GNSS particularly for Defence assets and civilian Systems of National Significance. • Use of BeiDou and GLONASS may present national security issues.

The compounding effects of the space weather event, the compromised GPS ground and space infrastructure, and potential compromise of interconnected cyber-physical systems, are found to potentially lead to moderate implications in the land, air, space and cyber domains (Figure 1). The maritime domain remains relatively unimpacted at this stage.

A system-wide cyber attack of PNT infrastructure has never occurred yet to public knowledge. Yet, ground stations lie at the nexus between the space and user segments of PNT, have a myriad of new and legacy hardware and software architectures, and may form the weakest link in the security of PNT infrastructure.[9] As such, the inject is assigned a threat likelihood rating of 2 at an optimistic level (Table 9). At this stage, moderate to minor consequences may be experienced across Defence, government, and the broader community.

Figure 1. Consequence mapping under Scenario 1 Inject 1, with 24-48 hour disruptions to GPS.



[9] https://spacenews.com/why-we-need-to-take-satellite-ground-station-security-seriously

Table 9. Risk matrix for Scenario 1 Inject 1.

Threat score: 2 **Consequence score: 2.67**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.2.2 Scenario 1 Inject 2

Scenario 1 Inject 2 explores a lack of sovereignty over critical enablers of national security and critical infrastructure, compounded by a short-term 24-hour GPS outage. Table 10 highlights participant responses to the inject, Figure 2 summarises the responses in a consequence map across Defence domains, and Table 11 analyses impacts in a risk matrix.

Table 10. Responses to Scenario 1 Inject 2.

Systems and services impacted
• Any system that requires 99.999% timing availability will be impacted. • Mobile services impacting communications networks will likely experience outages. • Weapons system capabilities are degraded though not necessarily offline. • Additional restrictions on military airspace and flight activities. • Naval positioning capabilities that were not impacted in Inject 1 will certainly be affected during a GPS outage. • Earth stations as a cyber attack surface. • Defence IT networks, related to Defence coordination and reporting. • Coordination of energy grid requiring sub-second time synchronisation. • Commercial off-the-shelf / Military off-the-shelf (COTS / MOTS) devices of US origin requiring GPS would be unserviceable.
Response and priorities
• Perform risk mitigation, request halt on training / operations • Use ground-based augmentation. • Prepare space-based augmentation systems for shut down, prioritising Safety-of-life systems. • Prioritise public safety and order, continuation of utilities, command and control for national security and Chief of Joint Operations-drive mission priorities • Potential shut down of the electricity grid for 24 hours and use of backup power generators (including warship capabilities) where possible.
Alternative systems or technologies
• GNSS constellations outside of GPS, for example switching from GPS to Galileo for 24 hours assuming users have dual receivers, ideally automatically. • Ground-based augmentation. • Commercial satellite systems that can provide independent timing. • Celestial and vision-based navigation. • RF (High Frequency) for timing and time distribution. These systems could be placed in in central locations to distribute time. • Rely on internal holdover clocks.
Issues with alternatives
• RF time can be used but is no longer good enough for energy, financial networks. • Even if systems are set up to switch from using GPS to Galileo, the time standard will change. • Internal holdover clock time can drift. • One network time will differ to another networks, presenting an interoperability issue. • Use of nominated alternatives presents an interoperability issue with other allied systems (Five-Eyes are assumed to use GPS). • Defence and critical infrastructure policies on use of multi-GNSS constellation are unclear.
Other considerations
• Given Australia's extensive dependence on GPS, it was unclear to what extent systems would be affected and the extent of the impact. • Depending on whether this event is considered a space issue, a cyber issue, or a geopolitical issue, the relevant authorities would communicate on the incident and priorities through relevant government channels. • Unclear on the process to communicate to all affected users if normal or backup communications channels are degraded.

This inject explored responses to a lack of PNT sovereignty and command and control, during which time a short-term 24-hour GPS outage is enforced out of necessity. By this stage, all domains would be heavily impacted including maritime (Figure 2). Concerningly, several of Defence's major systems and networks would be unserviceable, including weapons systems, shared allied systems, and Defence IT networks on which logistics and health planning capabilities are hosted. Loss of many critical services is attributed to loss of time synchronisation, which then becomes a pressing Defence and national issue with no viable scalable alternative.

The threat likelihood is given a rating of 'Highly Unlikely', as the GPS constellation and service as-a-whole has never been reset, as described in the inject. Consequences across the different critical factors are assigned ratings of Major to Severe.

Figure 2. Consequence mapping under Scenario 1 Inject 2, with additional 24-48 hour anticipated outage of GPS and handling of a cross-jurisdictional cyber-attack impacting Australia.

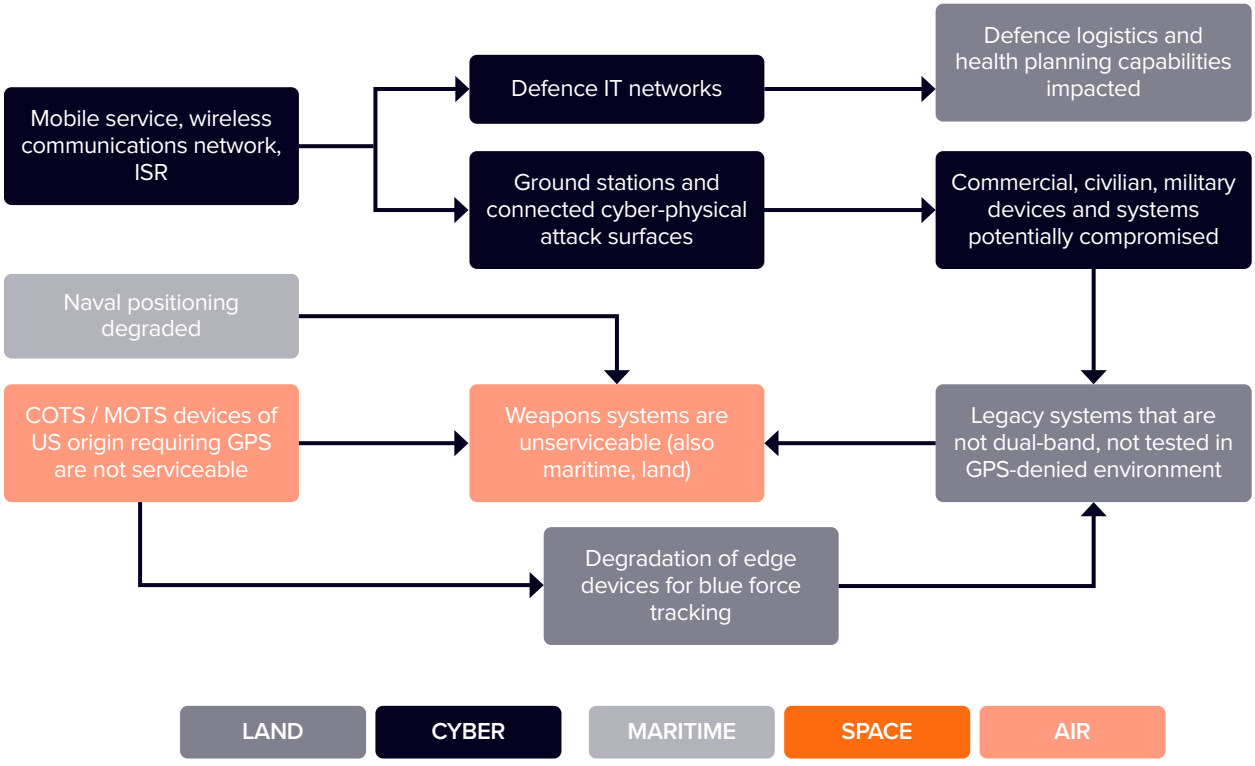


Table 11. Risk matrix for Scenario 1 Inject 2.

Threat score: 2 **Consequence score: 4.33**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National-level governance and decision-making mechanisms are degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems are degraded. Governance and decision-making mechanisms are somewhat impaired at the national-enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.2.3 Scenario 1 Inject 3

Scenario 1 Inject 3 involves a non-kinetic attack in-orbit, contributing to longer-term blanket GPS outage. Table 12 highlights participant responses to the inject, Figure 3 summarises the responses in a consequence map across Defence domains, and Table 13 analyses impacts in a risk matrix.

Table 12. Responses to Scenario 1 Inject 3.

Systems and services impacted
• Exposed systems beneath the EM pulse including LEO satellites. • Defence IT networks. • Defence grids are connected to national grids, and if the national grid is unavailable, then Defence's primary source of power would be unavailable. Defence's ability to project power, and our defensive and offensive capabilities, would be impacted. • Aviation and supply chains. • Impact on life support systems becomes critical during extended outages.
Response and priorities
• Change in national setting from crisis to conflict which underpins prioritisation and interoperability. • With regards to the ANZUS Treaty, an attack on US systems could affect Australian Defence posture.
Alternative systems or technologies
• Unencrypted communications, including RF communications and traditional approach of relaying messages / communications. • Navigation and timing that does not rely on GPS. • If not all GPS satellites are affected by the EM pulse, there is the potential to use GEO satellites to link and transmit timing signals from operational satellites. For example, using SBAS for time synchronisation, even though there is no immediate capability. • LEO systems to relay time. • Wide Local Area Network communications. • Use commercial systems where possible, e.g. Inmarsat in GEO, Iridium in LEO, Locata on the ground. • Use ground-based L1/L2 transmitters. • Potential to use signals of opportunity from LEO satellites (e.g. Starlink), but are currently low Technology Readiness Level research projects.
Issues with alternatives
• LEO systems could be an alternative to relay time, but they are less hardened and could be impacted by the EM pulse as well. • Ground-based PNT transmitters are viable, but limited by their line of sight.
Other considerations
• There is no clear authority for restoration of PNT services in Australia. • SouthPAN is not set up or resourced to support national-scale PNT crises.

Critical infrastructure services on which Defence relies on would be severely impaired, including the national grid, fuel supply, and logistics. By this stage, the national posture may shift from crisis to conflict, exacerbated by a loss of social cohesion (Figure 3).

The threat likelihood is given a rating of 'Highly Unlikely' (Table 12), as a non-kinetic attack in-orbit of the scale postulated in the inject has not occurred yet. This is an optimistic rating, and the threat likelihood could be escalated to 'Realistic Probability' for the following reasons:

- Anti-satellite tests have been carried out by nations previously, though not as part of warfare.
- There have been significant allegations of a Russian program developing nuclear counter space weapons.

Figure 3. Consequence mapping under Scenario 1 Inject 3, with extended outage of GPS.

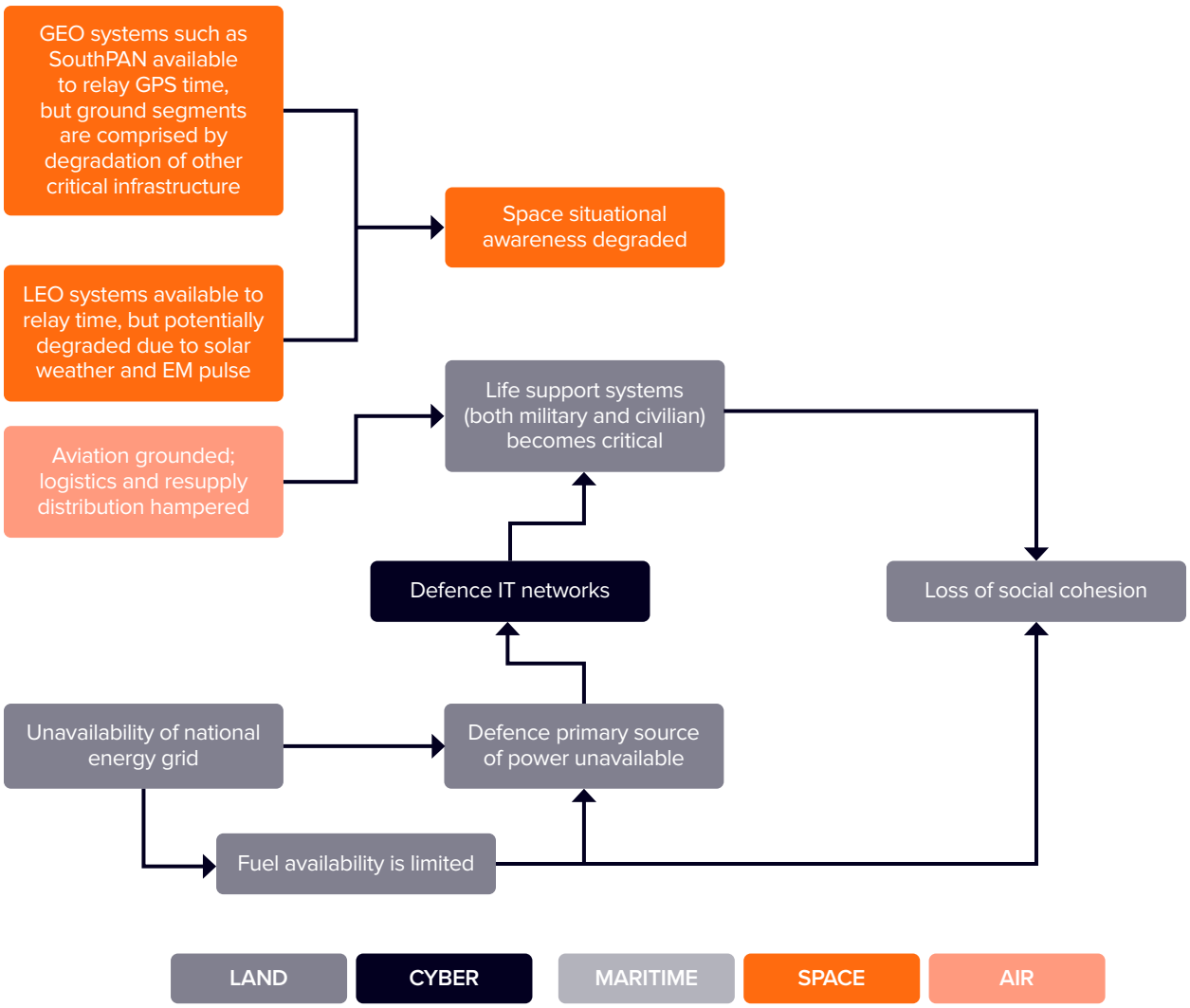


Table 13. Risk matrix for Scenario 1 Inject 3.

Threat score: 2 **Consequence score: 5**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.3 Responses to Scenario 2

3.3.1 Scenario 2 Inject 1

Scenario 2 Inject 1 involves a joint military exercise with live missile firing, in an environment with intermittent GPS jamming. Table 14 highlights participant responses to the inject, Figure 4 summarises the responses in a consequence map across Defence domains, and Table 15 analyses impacts in a risk matrix.

Table 14. Responses to Scenario 2 Inject 1.

Systems and services impacted
• Navigational capabilities may be degraded if civilian GPS signals are degraded. • Degraded targeting and missile firing. • Loss of navigational situational awareness for both Defence and civilian ships in the vicinity of the exercise area, such as commercial air and surface vessels. • Potential intelligence loss for Defence and increased intelligence for the adversary. • Onboard systems requiring timing from GPS, especially industrial control systems, ranging from air conditioning units to sewerage, and that are essential for keeping other systems in operation. • Civilian radar when used by Defence ships for navigational backup and coverage.
Response and priorities
• Perform risk analysis and only proceed with the exercise with caution. • Possible to use this situation as an opportunity to continue exercises under a denied GPS environment.
Alternative systems or technologies
• Visual line of sight for some maritime activities (but not weapons and high-risk activities). • More accurate / precise inertial navigation systems on warfighting platforms. • Navigational radar. • Use of military GPS, if not affected. • VHF voice radio for communicating PNT information.
Issues with alternatives
• Line of sight can only be used during daytime operations and can be affected significantly by weather conditions such as fog and rain. • Inertial units will drift over time. • Navigational radar has limited range and emits active signals making the ship detectable to enemy forces. • VHF communications also have limited range and are susceptible to interception by enemy forces.
Other considerations
• Re-evaluate risk assessment, and check policy compliance and/or government risk appetite to continue exercises in a GPS denied environment.

Although the direct impact appears primarily limited to the maritime domain, loss of situational awareness with some potential for commercial collateral may be experienced in the cyber and air domains respectively (Figure 4).

The threat likelihood is assigned a rating of 'Likely or Probable' (Table 15). Defence has not publicly reported encountering the high levels of jamming during military exercise, as those observed in other conflict zones.

However, indiscriminate GPS jamming has been reported to occurred in the northern waters of Australia impacting commercial aviation. Thus, the threat remains credible, and the likelihood of grey zone activities in the region is likely. In this inject, the quality of the joint exercise may be diminished, though generally impacts remain minor. As such, moderate to minor consequence ratings are assigned across the critical factors.

Figure 4. Consequence mapping under Scenario 2 Inject 1, with intermittent jamming impacting military exercises.

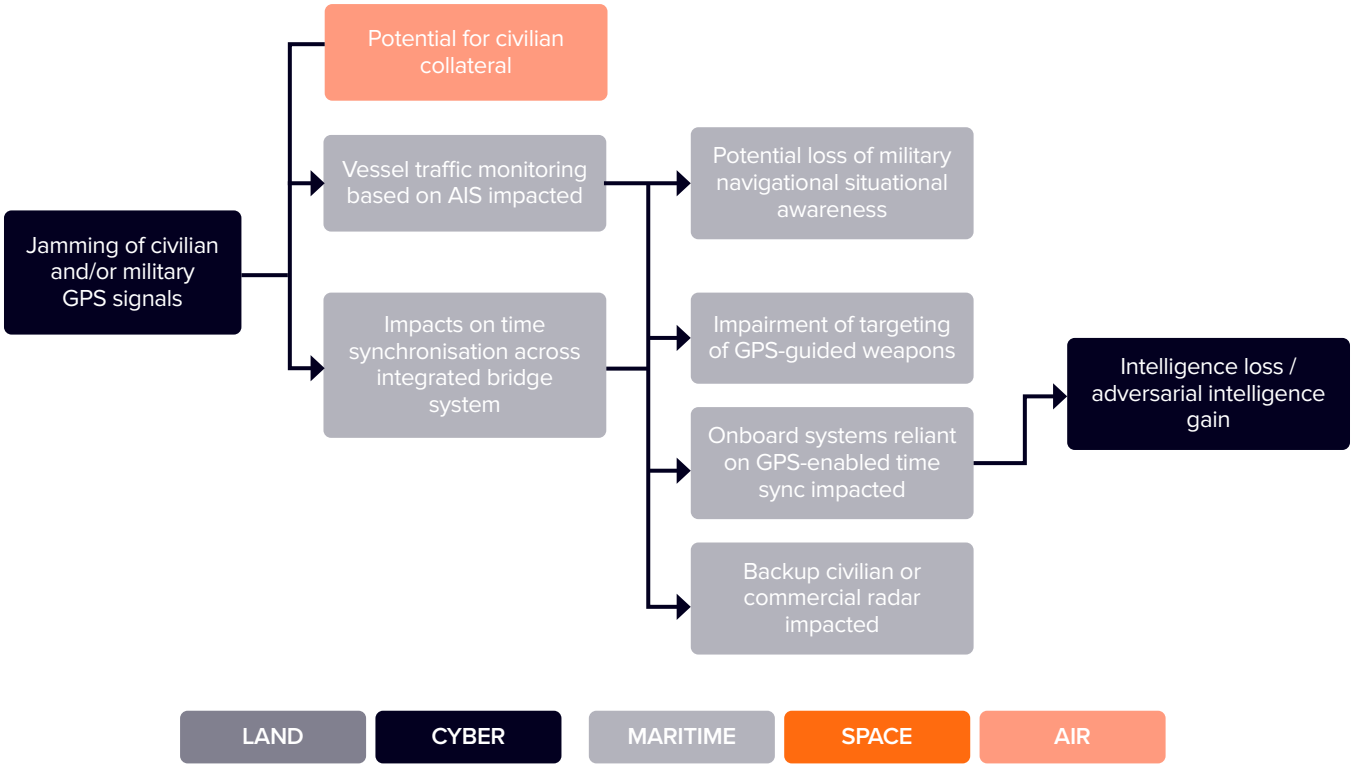


Table 15. Risk matrix for Scenario 2 Inject 1.

Threat score: 4 **Consequence score: 2.33**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.3.2 Scenario 2 Inject 2

Scenario 2 Inject 2 diverts the fleet towards a search and rescue mission, in an environment with persistent jamming causing degraded GPS signals. Table 16 highlights participant responses to the inject, Figure 5 summarises the responses in a consequence map across Defence domains, and Table 17 analyses impacts in a risk matrix.

Table 16. Responses to Scenario 2 Inject 2.

Systems and services impacted
• EPIRB (Emergency Position-Indicating Radio Beacon) is not as effective without GPS signals. • Search and rescue capability is hindered. • Ability to identify and coordinate response activities is impaired. • Civilian air and sea situational awareness is impacted. • Use of e-Navigation hindered. • Overall ships and planes should still be able to navigate to a point without GPS.
Response and priorities
• Perform risk analysis and proceed with the exercise only when it is deemed appropriate.
Alternative systems or technologies
• Use of inertial sensors. • RF localisation from space. • Use of Earth Observation capabilities to supplement navigation. • Radar for search and rescue. • Voice coordination of search. • Visual navigation. • Use of VHF.
Issues with alternatives
• Alternatives are unable to transmit time. • Visual navigation can only be used during day time operations and can be affected significantly by weather conditions such as fog and rain • Inertial units will drift over time • VHF comms also have limited range and are susceptible to interception by enemy forces.
Other considerations
• Avoid use of offensive measures where possible. • Possibility to proceed with non-escalatory search and rescue even in a degraded environment, pending risk assessment and acceptance. For example, aircraft can observe and clear airspace, then helicopter can fly over rather than through jammed area.

The disruption is anticipated to impair primarily the maritime domain (Figure 5), causing loss of automated navigational capabilities and situational awareness. Aviation assets supporting the search and rescue mission are expected to also be affected by the jamming with potential for degradation of air domain awareness.

The threat likelihood is assigned a rating of 'Highly Likely' (Table 17), as GPS jamming occurs on a regular basis globally and is almost expected in conflict areas. While the likelihood of the threat is high, the overall impact to ADF operations, affected domains, and public perception and safety is qualitatively assessed as moderate, with some civilian collateral effects anticipated.

The consequences of the threat are partly mitigated by the proficiency of naval personnel in traditional and alternative methods for navigation. However, the same reliable backups are either unavailable or not applicable in other domains, such as air operations. Additionally, the loss of GPS-enabled time synchronisation cannot be readily replaced by traditional methods.

Figure 5. Consequence mapping under Scenario 2 Inject 2, with search and rescue hampered by persistent GPS jamming.

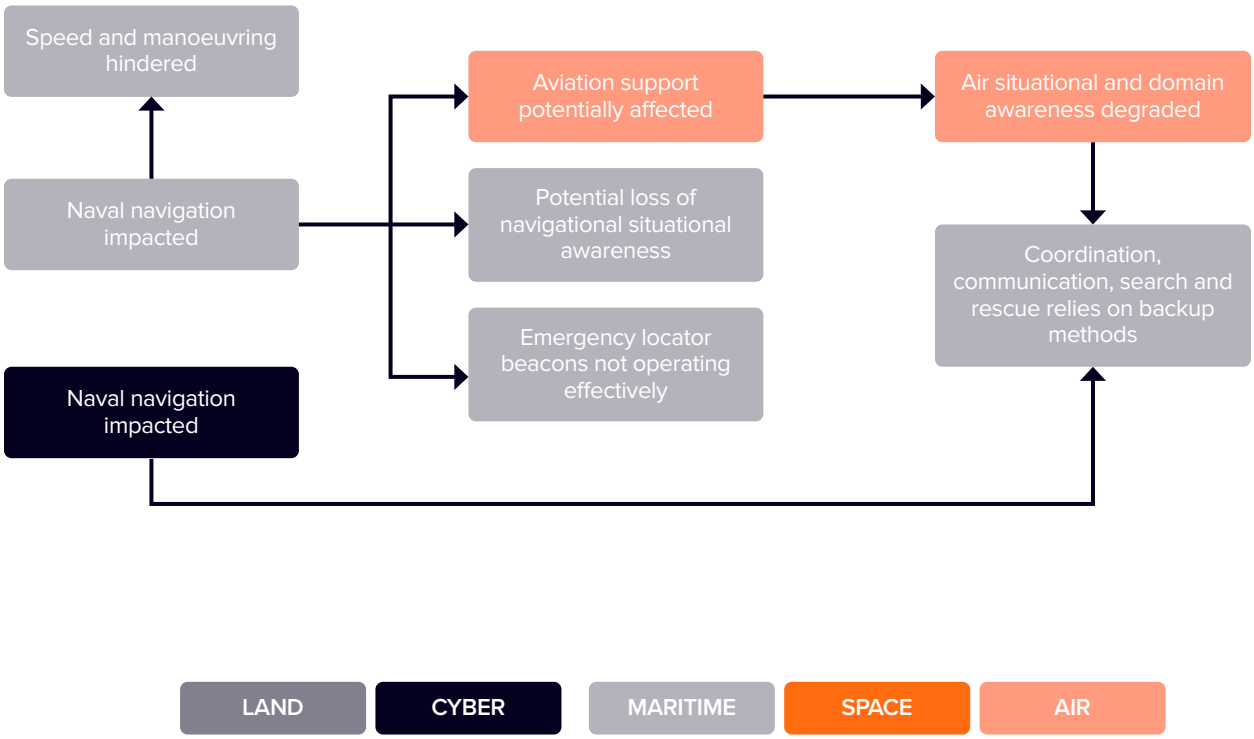


Table 17. Risk matrix for Scenario 2 Inject 2.

Threat score: 5 **Consequence score: 3**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.3.3 Scenario 2 Inject 3

Scenario 2 Inject 3 directs the fleet to support allied troops, however efforts are hampered by long-range GPS spoofing. Table 18 highlights participant responses to the inject, Figure 6 summarises the responses in a consequence map across Defence domains, and Table 19 analyses impacts in a risk matrix.

Table 18. Responses to Scenario 2 Inject 3.

Systems and services impacted
• Weapons and combat systems. • Radar systems. • Advice to other vessels. • Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) systems. • Navigation and location systems. • Inability to defend fleet against incoming munitions. • One ship impacted during spoofing could be due to system differences, location differences, or operator knowledge of a threat or issue.
Response and priorities
• Consideration of whether an electronic attack constitutes escalation within conflict. • If attribution of the spoofing source leads to an increase in conflict level, then it may be necessary to modify the posture and strategy of the ships and fleet.
Alternative systems or technologies
• Use of other unaffected GNSS, such as Galileo. • Revert to dead reckoning for navigation. • Nautical charts and traditional navigation methods including stenography and shorthand; bathymetric mapping and navigation by features. • Satellite communications. • Communications from other vessels to advice on threats; integrated reports across ships to identify and characterise the error. • Emerging technologies like quantum-based timing could help where precision PNT is needed for effective use and access to weapons systems. • Terrestrial-based systems for aviation. • Visual, e.g. launch aircraft to explore “boundaries” of the affected signal. • Celestial navigation. • Use anti-spoof GNSS receivers or capabilities.
Issues with alternatives
• Quantum based timing technologies are in early TRL stages • Not many defence staff are skilled in traditional navigation techniques such as the use of sextants for celestial navigation • Anti-spoof receivers, whilst much better protection against spoofing, can still be affected.
Other considerations
• Defence constraints in employing alternative technologies include costs in implementing and effort to scale. • Plug and play output of the alternative technology must match the original output for interoperability reasons. • Militaries need agreements to use military PNT (ITAR issues).

The disruption is expected to impair C5ISR coordination with allies including in the air and land domains, compromise fleet security and domain awareness, and jeopardise mission objectives (Figure 6).

The threat likelihood is assigned a rating of 'Likely or Probable' (Table 19), due to the precedence of electronic warfare occurring in situations of conflict.

A 'Moderate' consequence rating is assigned across the critical factors, reflecting impaired coordination and communication across the fleet and rising public awareness and concern of the situation. Consequence rating of Defence situational awareness may in some cases be escalated to 'Likely or Probable', as GPS spoofing represents a shift into the conflict spectrum.

Figure 6. Consequence mapping under Scenario 2 Inject 3, with a coalition call for ADF support hampered by long range spoofing.

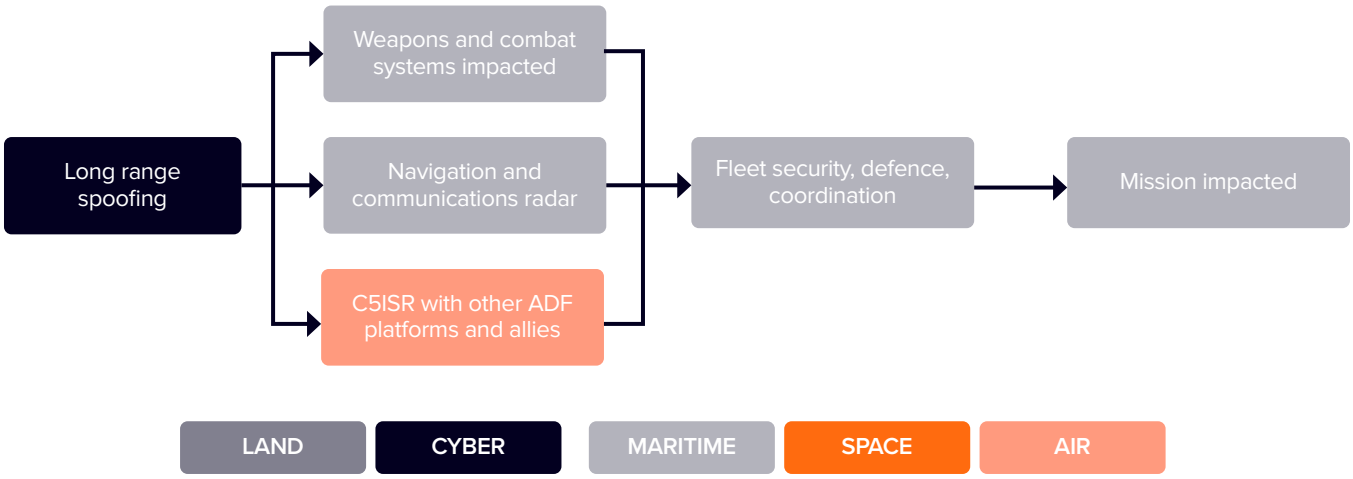


Table 19. Risk matrix for Scenario 2 Inject 3.

Threat score: 4 **Consequence score: 3**

Threat (Score)	Likelihood Description	Consequence (Score)	Critical infrastructure and ADF operations	Defence situational awareness	Public perception and safety
Highly Likely (5)	Threat to PNT occurs often (i.e. weekly to daily in frequency); intentional; adversary has capability.	**Severe (5)**	Ability to coordinate and communicate is disabled. Enterprise operations and social systems are not functioning. Governance mechanisms are disabled at the national level. National security is significantly compromised.	C5ISR through all Defence domains are disabled. Far right on the conflict spectrum. National threat alert may be advising certainty of further threats.	Loss of social cohesion. Loss of life. Defence required to restore civil unrest.
Likely or Probable (4)	Threat to PNT occurs on a frequent basis (i.e. monthly in frequency); intentional; adversary has capability.	**Major (4)**	Degraded ability to coordinate and communicate. Enterprise operations and social systems are overwhelmed. National to enterprise level governance and decision-making mechanisms may be degraded.	C5ISR through 3-5 Defence domains are disabled. Right on the conflict spectrum. Mission objectives cannot be realised. National security is compromised. Significant structural adjustment required to respond to threat.	Insecurity amongst the public. Significant loss of confidence in government to manage and contain the impacts. There may be fatalities and serious casualties. Defence required to restore civil unrest.
Realistic Probability (3)	Threat to PNT occurs infrequently (once to several times before); may be intentional or unintentional depending on context.	**Moderate (3)**	Coordination and communication are hindered and cannot be conducted through usual means. Enterprise operations and social systems may be degraded. Governance and decision-making mechanisms are somewhat impaired at the enterprise level.	Impact from the threat is not contained. Grey zone activities have degraded C5ISR impacting 3-4 Defence domains and quality of operations. Some loss of situational awareness. Mission objectives may be compromised.	Marked and sustained interest, concern expressed by increasing numbers of the public. Impacts may lead to several casualties.
Highly Unlikely (2)	Threat to PNT may not have occurred previously. Adversarial capability exists but not used yet.	**Minor (2)**	Coordination and communication are hindered or cannot be done through usual means. Enterprise operations and social systems experience minor impact. Enterprise-level governance and decision-making functions are impacted.	Minor impact on 1-2 Defence domains. C5ISR degraded though still possible with alternative methods. Grey zone on the conflict spectrum. Minor impact on quality of operations or achieving mission objectives.	Interest raised, no marked concern. Impacts may lead to several minor casualties but no fatalities.
Remote Chance (1)	Threat to PNT has no precedent. Little intent nor adversarial capability to pose threat. Consequential natural PNT threat not anticipated in the foreseeable future.	**Insignificant (1)**	Impact on the ability to coordinate and communicate is inconsequential. Enterprise operations and social systems can cope with changes. Decisions can be escalated through existing governance and decision-making functions.	Inconsequential impact on domains. Inconsequential impact on quality of operations or achieving mission objectives. Situational awareness maintained.	Public interest mitigated. May cause minor injuries with no long-term consequences.

3.4 Risk and Resilience

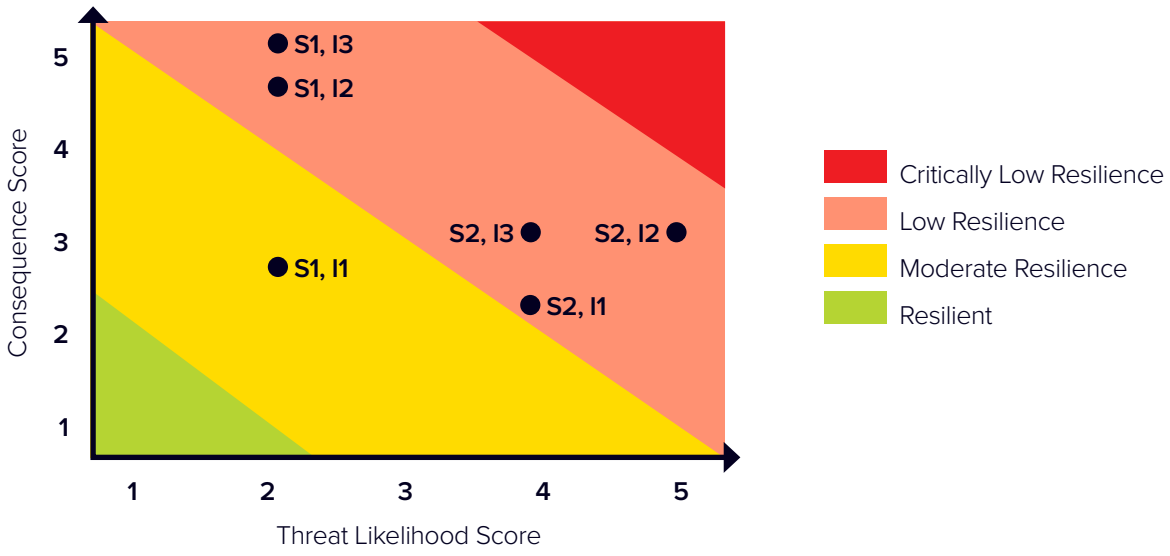
The 6 injects are summarised in terms of their normalised threat and consequence scores (Table 20), and mapped on a threat-consequence plot (Figure 7). The plot is not intended to imply correlation or causation, but rather to qualitatively compare and contrast the resilience of Defence, government, and the nation as a whole to various PNT disruptions. Indeed, the consequence scores could be interpreted as PNT resilience scores.

Note that the threat and consequence scores are subjective, influenced by the specific injects and the critical factors chosen for assessment. Nevertheless, this mapping offers some insight on the PNT threats and the magnitude of their consequences.

Table 20. Summary of injects and their respective threat and consequence scores.

Scenario, Inject	Description	Threat Score	Consequence Score
S1, I1	Space weather + opportunistic cyber hack on GPS master ground station	2	2.67
S1, I2	GPS to be reset	2	4.33
S1, I3	Non-kinetic attack in-orbit delays GPS reset process	2	5
S2, I1	Intermittent GPS jamming experienced during military maritime exercise	4	2.33
S2, I2	Persistent GPS jamming during search and rescue mission	5	3
S2, I3	GPS spoofing experienced during operational mission	4	3

Figure 7. Plot of the 6 injects on the threat-consequence plot to compare the PNT resilience of Defence, government, and the broader nation during different situations of PNT disruption.



Moving towards a resilient posture in Scenario 1

Where the threats are highly unlikely with little precedent, the corresponding consequence scores may be higher (score of 4-5), reflecting lower resilience to manage PNT disruption if these threats occurred. This is exemplified by the second (S1, I2) and third (S1, I3) injects of Scenario 1, which eventuated in prolonged outage of GPS lasting several days. These injects highlight the lack of preparedness within Defence, and more broadly, across Australia to address such significant threats.

The cyber and non-kinetic threats in Scenario 1 were directed towards non-sovereign PNT assets and infrastructure (i.e. US-owned assets). For Defence to move its posture in (S1, I2) and (S1, I3) from the "Low Resilience" segment towards the "Moderate Resilience" segment, it would be more effective to take actions to decrease the consequence score rather than the threat likelihood score. This could be done through:

- Undertaking a comprehensive PNT audit to evaluate and characterise Defence's PNT-dependent systems (Section 4, **Recommendation 1**);
- Nominating a national backup time reference (Section 4, **Recommendation 2**).

To start shifting S1, I1 from the "Moderate Resilience" towards the "Resilient" level, one potential action could be to:

- Develop a GPS integrity monitoring capability (Section 4, **Recommendation 3**).

Moving towards a resilient posture in Scenario 2

Where the threat is highly likely, characterised by precedence, malicious intent, and adversarial capability (such as targeted GPS jamming and spoofing in a maritime environment), the corresponding consequence score may be lower (score of 2-4). This may reflect Defence's capability to manage their response in certain situations. In a maritime environment, naval vessels losing access to civilian GPS signals temporarily may not present major issues – naval personnel have long relied on traditional and alternative methods. This becomes more challenging when: i) mission-critical operations involve coordination between maritime, land and air domains; and ii) weapons systems readiness is required for domain awareness and security. Both requirements depend, sometimes exclusively, on GPS for their PNT needs.

The spoofing and jamming threats in Scenario 2 were directed towards Defence assets and systems, representing deliberate actions by an adversary to disrupt Australia missions through grey zone and overt hostilities. To shift Defence's resilience posture in Scenario 2 from the "Low Resilience" segment towards the "Moderate Resilience" segment, Defence should focus on both addressing the threat and mitigating the consequences. This could be done through:

- Development of a multi-source, multi-layered PNT architecture and capability. This would assure access to PNT and hence deter the threat of PNT denial by adversaries through jamming and spoofing (Section 4, **Recommendation 4**).
- Undertaking scenario planning and testing during military operations where GPS is actively disabled to identify, respond to, and mitigate vulnerable systems (Section 4, **Recommendation 5**).
- Elevating of spoofing threats and anti-spoofing capabilities to both the Defence and national agenda (Section 4, **Recommendation 6**).
- Expanding and standardising training in traditional methods of navigation across domains (Section 4, **Recommendation 7**).

Finally, there has been significant Defence and government investment in emerging quantum technologies, including for PNT. These investments include the AUKUS Quantum Arrangement,[10] Advanced Strategic Capability Accelerator's Emerging Disruptive Technologies Program,[11] and the Critical Technologies Challenge Program.[12] However, a key challenge is the ad-hoc development of these technologies for warfighting assets, or to stimulate industry growth, without a cohesive PNT strategy that ensures interoperability with other supporting and critical legacy systems. While assured PNT is essential for tactical platforms, it is equally crucial for the critical infrastructure sectors that Defence depends on. There needs to be a designated authority, such as a National PNT Office, to coordinate these initiatives within a cohesive national agenda (Section 4, **Recommendation 8**).

[10] https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf
[11] www.minister.defence.gov.au/media-releases/2024-11-18/albanese-government-invests-australian-innovation-give-defence-technological-edge
[12] https://business.gov.au/grants-and-programs/critical-technologies-challenge-program/grant-recipients

3.5 Additional operational contexts for PNT

Workshop participants provided feedback on Scenario 2, noting that cascading impacts from PNT would be more extensive in situations requiring increased air support or time-critical missions in GPS-denied environments. These challenges would demand a more deliberate and coordinated participant response. These suggestions have been developed and presented as vignettes for future consideration.

Vignette 1 below could be designed to evaluate Defence's response to PNT disruption in the context of a foreign nation expanding its infrastructure and soft power, potentially escalating tension in the Indo-Pacific region. It also highlights the foreign nation's potential technological superiority, creating an asymmetric advantage over Australia.

Vignette 1

The ADF is undertaking a humanitarian assistance operation across multiple islands in the South Pacific, involving coordinated efforts by the Army, Navy, and Air Force. The operation faces significant challenges due to a severe geomagnetic storm disrupting GPS services. A rising regional competitor offers island leaders access to their satellite navigation services for humanitarian purposes, proposing to rapidly set up additional ground stations within the premises of their Pacific embassies. Furthermore, the competitor pledges to supply receivers compatible with their satellite services to support the effort.

Vignette 2 could be designed to disrupt routine operations by affecting air support in a GPS-degraded environment, while also highlighting contemporary concerns about broader security implications.

Vignette 2

The RAAF is conducting routine logistics air support for an Antarctic resupply mission on behalf of the Australian Antarctic Division. Mid-operation, the aircraft is tasked with diverting to assist in a maritime vessel search and rescue effort, including supporting safety of navigation through ice-covered seas. During the mission, GPS signals are disrupted by an unidentified source. Evidence suggests deliberate interference by a foreign power seeking to assert influence over strategic routes in the Southern Ocean, and competition over Antarctica. The disruption complicates the operation and raises concerns about broader security implications.

4
RECOMMENDATIONS

This section contains recommendations based primarily on workshop participant responses and analyses of the scenario planning exercises. The recommendations should be in place for Defence resilience, though not all initiatives need to be led by Defence. Note that these recommendations are intended to stimulate discussion. Any further considerations of prioritisation, progressions, and investment in recommendations should be supported by additional validation beyond the scope of this report.

1	National PNT audit based on cyber security frameworks
Challenge	Participants acknowledged the lack of national understanding of systems that rely on GPS, and cascading impacts on dependent systems.
Recommendation	Conduct a comprehensive PNT audit, based on cyber security risk management frameworks, to evaluate and characterise Defence's PNT resilience profile at the enterprise level.
Rationale	A PNT audit based on practical and applicable cyber security frameworks – such as the National Institute of Standards and Technology to Identify, Protect, Detect, Respond, and Recover – would enable a comprehensive, systematic, and scalable approach to addressing PNT risks to Defence. The audit should include an assessment of GPS dependencies in systems outlined in the Defence Integrated Investment Program, enabling Defence to better prioritise, sequence and harden capabilities. The audit would also guide Defence in replanning for redundancy and fallback strategies in military operations. Additionally, the audit should extend to civilian critical infrastructure, including mapping key business and operational systems that Defence depends on.

2	Designate a national backup time reference
Challenge	While several alternative PNT systems or technologies are potentially available, they often face interoperability and integration issues, particularly concerning time synchronisation (refer to Section 3.2.2 – Issues with Alternatives).
Recommendation	Designate a national backup time reference or network clock to enable both Defence and critical infrastructure systems to synchronise and connect to in a prioritised manner.
Rationale	Backup timing approaches exist (use of RF to transmit time, internal holdover clocks, network time, non-GPS GNSS), however these are prone to time drift and/or make use of a different time standard. For essential Defence, government, and business operations to continue, it will be important for Defence and Australia designate a national backup time. In parallel, this must be complemented with the development of the TTPs to transmit and communicate reference time in a repeatable, reliable and achievable way to government, businesses and the broader community.

3	GPS integrity monitoring and operational safeguards
Challenge	Participants highlighted concerns about using degraded GPS signals for Defence and critical infrastructure systems until the integrity of GPS can be assured and ensured.
Recommendation	Develop a robust national capability for GPS signal integrity monitoring and assurance, to identify, detect and respond to the loss of integrity of GPS signals.
Rationale	Inherent in this capability is the need for operator training to detect and characterise GNSS signal degradation. Operators of critical infrastructure should also have the ability to manually override systems and switch to alternative timing sources where necessary. This safeguard would support at least a baseline level of operational continuity until GPS integrity can be assured. Through a Factsheet for PNT, the Department of Home Affairs has highlighted risk to PNT as a potential material risk to critical infrastructure sectors, urging operators to consider various forms of PNT redundancy. With regards to Defence, the ability to manually override systems depends in part on established policies and security protocols with allied systems. It may be prudent to re-evaluate these arrangements in considering the increasing probability of large-scale GPS disruption or denial.

4	Multi-layered PNT architecture and capability
Challenge	Australia's reliance on a primary space-based constellation for its PNT needs (i.e. GPS) creates significant vulnerabilities for national security and resilience.
Recommendation	Develop a multi-source, multi-layered PNT architecture and capability to address the vulnerabilities of Defence reliance on GPS for its PNT needs.
Rationale	This multi-layered capability could include: • a terrestrial timing system capable of transmitting time signals (such as eLORAN); and • a multi-orbit satellite system that complements GPS and/or GNSS and provides hardened navigation and timing signals to enhance resilience against disruption. Defence's recent emphasis on resilient multi-orbit satellite communications capabilities may provide an opportunity to integrate co-located PNT capabilities, enhancing overall communications and PNT resilience.

5	Scenario planning, testing and training in a GPS-denied environment
Challenge	Participants noted that the full extent of maritime (and other domain) system vulnerabilities to GPS disruptions remain unclear.
Recommendation	Undertake scenario planning, testing and training exercises across all domains, in environments where GPS is actively disabled, to identify, respond to, and mitigate vulnerable systems.
Rationale	These exercises should go beyond merely testing the performance of alternative technologies or testing one or two systems under strain. Instead, the exercises should involve actively disabling access to GPS to uncover previously unrecognised impacts. It is prudent to proactively to plan for scenarios across the conflict spectrum – from peacetime to grey zone activities to contested environments. This would enable a comprehensive re-evaluation of PNT risks and navigation warfare threats across all domains and the development of effective mitigation strategies.

6	Elevate official discussions on anti-spoofing
Challenge	Defence rules of engagement and publicly available information do address restrictions to the electromagnetic spectrum, such as jamming by adversaries. However, spoofing receives far less attention and possibly represents a gap in Defence's consideration of electronic warfare. Unlike jamming, which can be construed as an adversary's right to self-defence or an unintentional act, spoofing is a deliberate effort by an adversary to deceive and mislead.
Recommendation	Elevate discussions on spoofing threats and anti-spoofing capabilities within the Defence and national security agendas, ensuring comprehensive strategies are developed to address PNT risk management as critical components of cyber and electronic warfare.
Rationale	Similar to the focus and recognition of GPS jamming as an electronic attack, it is essential to consider spoofing as a PNT threat and anti-spoofing capabilities. This would ensure electronic protection systems are adequately prepared to counter, and thus deter, deliberate PNT deception efforts.

7	Expand and standardise training in traditional and alternative techniques
Challenge	The Navy employs manual, non-GNSS navigation techniques during training, such as celestial navigation using star observations. However, it remains unclear whether these methods have practical applications beyond training, whether they can be scaled effectively, or if they can be used as a reliable alternative for mission-critical operations.
Recommendation	Expand and standardise training in traditional and alternative PNT techniques as an effective stop-gap measure, ensuring that personnel across multiple domains are Trained and Equipped to navigate and communicate in EMS-contested environments.
Rationale	Traditional and alternative navigation methods are an essential stop-gap measure while emerging technologies for assured PNT or precision navigation are not at the maturity levels needed for operational resilience. Additionally, these methods are necessary to ensure Defence readiness for contingency scenarios where PNT access cannot be readily assured.

8	Establish a National PNT Office
Challenge	It is evident that Australia lacks a central authority for resilient PNT. Compounding the challenge is that PNT is a major responsibility with various complexities that may not fall solely under the purview of any single government department.
Recommendation	Establish a designated authority, such as a National PNT Office, to coordinate PNT initiatives across relevant government agencies, including Defence, a create a cohesive national agenda aimed at enhancing PNT resilience.
Rationale	In the past 12 months, there has been significant government investment in emerging technologies with a quantum focus. In relation to PNT, these investment initiatives include the AUKUS Quantum Arrangement, ASCA Emerging Disruptive Technologies, and DISR Critical Technologies Challenge. What is lacking is the framework (PNT strategy / office), rollout to and integration with legacy systems. The most significant challenge in addressing these issues is lack of clear policy, investment, and accountability for several of what would be national initiatives, and not constrained to ad-hoc technology development alone.

5
CONCLUSION

A scenario planning exercise at the OFFICIAL level tested Defence's response to a series of injects involving escalating GPS outages and conflict scenarios. The scenarios involved natural, cyber, and non-kinetic hazards, with emphasis on potential realities occurring in the space, cyber, and maritime domains. Findings from the exercise revealed that while Defence could manage responses to GPS disruptions caused by space weather hazards, overall PNT resilience remains low when facing more deliberate threats to PNT. To improve its resilience posture, Defence must address both the likelihood of PNT threats and the severity of their consequences. Doing so would enable Defence to shift from a low resilience to moderate and/or fully resilient PNT threat readiness level. Major challenges for Defence are:

- Lack of understanding of the extent of its GPS-dependent systems.
- Interoperability and/or integration issues in using alternative PNT systems or technologies to GPS, particularly concerning time synchronisation.
- Lack of capability to ensure the integrity of GPS signals, raising concerns about the reliance on degraded GPS signals for Defence and critical infrastructure.
- Australia's reliance on GPS for its PNT needs.
- Uncertainty of vulnerabilities in situations of both intermittent to persistent GPS denial.
- Lack of definition of spoofing as an intentional, sophisticated PNT threat.
- Ambiguity around whether alternative or traditional methods of navigation have practical application beyond training, and beyond the maritime domain.
- Lack of a central authority to coordinate and lead efforts to increase PNT resilience.

This paper makes the following recommendations:

1. Conduct a comprehensive PNT audit, based on cyber security risk management frameworks, to evaluate and characterise Defence's PNT resilience profile at the enterprise level.
2. Establish a designated national backup time reference or network clock to enable both Defence and critical infrastructure systems to synchronise and connect to in a prioritised manner.
3. Develop a robust national capability for GPS signal integrity monitoring and assurance, to identify, detect and respond to the loss of integrity of GPS signals.
4. Develop a multi-source, multi-layered PNT architecture and capability to address the vulnerabilities of Defence reliance on GPS for its PNT needs.
5. Undertake scenario planning, testing and training exercises across all domains, in environments where GPS is actively disabled, to identify, respond to, and mitigate vulnerable systems.
6. Elevate discussions on spoofing threats and anti-spoofing capabilities within the Defence and national security agendas, ensuring comprehensive strategies are developed to address PNT risk management as critical components of cyber and electronic warfare.
7. Expand and standardise training in traditional and alternative PNT techniques as an effective stop-gap measure, ensuring that personnel across multiple domains are Trained and Equipped to navigate and communicate in EMS-contested environments.
8. Establish a designated centralised authority, such as a National PNT Office, to coordinate PNT initiatives across relevant government agencies, including Defence, a create a cohesive national agenda aimed at enhancing PNT resilience.

APPENDIX: RELEVANT LITERATURE

Table 21. List of relevant literature in providing context for this project.

Title	Description and relevance to PNT	Reference
Security of Critical Infrastructure Act	Regulates Australian critical infrastructure on risk management and cyber security obligations.	www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018
Critical Infrastructure Security Centre Factsheet for Critical Infrastructure on Positioning, Navigation and Timing	Provides high-level guidance to critical infrastructure operators on PNT risks and mitigation steps.	www.cisc.gov.au/resources-subsite/Documents/pnt-factsheet.pdf
Critical Infrastructure Security Centre Critical Infrastructure Annual Risk Review	Highlights risks to PNT such as from space weather.	www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf
Australian Cyber Security Strategy	No reference to PNT as a cyber issue.	www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
Bureau of Meteorology-Trusted Information Sharing Network Space Weather Fact Sheet	Outlines space weather as a natural hazard to PNT.	www.sws.bom.gov.au/Products_and_Services/5/18
AUKUS Quantum Arrangement	Arrangement under AUKUS Pillar 2 to accelerate investments in quantum technologies including PNT	https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf
Critchley-Marrows and Verspieren (2023). Ensuring PNT resilience: A global review of navigation policies and roadmaps.	Review and comparison of international PNT policies and roadmaps up to June 2023.	https://stig.pp.u-tokyo.ac.jp/stig/wp-content/uploads/2023/07/Resilient_PNT_Policy_Report_FINAL_ONLINE.pdf
Critchley-Marrows et al. (2024). A Time and A Place for Resilience.	Recommendations for government policy to better support the use of PNT services in the Australian economy.	https://frontiersi.com.au/wp-content/uploads/2024/02/FrontierSI_ResilientPNT_Report.pdf
Lee (2024). Resilient PNT for Disaster Response.	PNT policy recommendations for all-hazards response.	www.spacegovcentre.org/_files/ugd/ed2eed_0c1bfdc1a6564fb2b4ea5d915fddb5ce.pdf

FRONTIER SI

We know where.

frontiersi.com.au