Primed for pressure:

A Preparedness, Resilience and Redundancy Scorecard

REPORT

John Coyne and Raelene Lockhorst

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

25 YEARS
2001–2026

JULY 2026

About the authors

Dr John Coyne is Director of ASPI's National Security Programs.

Raelene Lockhorst is Deputy Director of ASPI's National Security Programs.

AI contributed no ideas to this report.

Acknowledgements

The authors extend their sincere thanks to the peer reviewers for their thoughtful comments, expert advice and constructive challenge, all of which significantly improved the quality of this report. We also thank the editorial team for their careful review, support and commitment to bringing this publication to fruition.

This report was produced with funding support from the Northern Territory Government. Responsibility for the content, findings and conclusions rests solely with the authors.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

About Reports

Reports deliver original and deeply researched analysis and judgements on issues of strategic significance and ongoing importance. Reports aim to inform and influence national strategic choices with original, deeply researched analysis that surfaces implications, tests assumptions, and may consider future courses of action.

First published July 2026
Published in Australia by the Australian Strategic Policy Institute
ISSN: 3083-2853 (Online), 3083-2861 (Print)

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Cover image: Defence image library, online.

Contents

Executive summary

Northern Australia now carries a strategic burden for the nation unmatched in the modern era. If deterrence fails, Australia's ability to project, sustain and recover combat power will depend on whether the north's enabling systems continue to function under pressure. Defence capability doesn't operate as a collection of isolated assets. A runway without fuel is a car park. A port without a maintenance workforce is a jetty. Operational effectiveness emerges from the interaction of fuel, logistics, infrastructure, workforce, digital systems and industrial capacity. When those systems function together, force posture delivers deterrence. When they fail, capability rapidly loses effect.

Australia has invested heavily in northern defence infrastructure, force posture and alliance integration over the past decade. Yet current assessment approaches still measure activity more effectively than readiness. Project delivery, expenditure and infrastructure growth show movement, but they don't reveal whether the broader system can absorb disruption, sustain operations or recover from cascading failure during a crisis.

Northern defence isn't a collection of isolated assets. It operates as an interconnected system in which failure in one domain rapidly affects others. Fuel disruption constrains logistics. Logistics degradation reduces sustainment. Digital disruption weakens coordination and decision-making. Workforce shortages slow recovery and regeneration. Under compound stress, vulnerabilities compound faster than traditional planning frameworks can capture.

The Preparedness, Resilience and Redundancy (PRR) Scorecard addresses that challenge. It provides a structured framework for assessing northern defence as a connected operational ecosystem rather than a series of stand-alone projects or capabilities. The framework measures three core dimensions:

1. *Preparedness:* the extent to which systems are ready before disruption occurs.
2. *Resilience:* the ability to absorb shock and continue operating under stress.
3. *Redundancy:* the existence of alternative pathways, backup capacity and surge mechanisms that prevent local disruption from becoming systemic failure.

This report applies the framework across nine domains organised into three operational tiers. Those domains span force posture and forward presence, logistics and sustainment, fuel and energy security, strategic infrastructure and estate, national support base, industrial base and regeneration capacity, digital, decision and command systems, integration with allies and partners, workforce and human capital. Together, they provide a system-level picture of where northern defence is robust, where it's fragile and where investment will generate the greatest operational effect.

Scenario testing demonstrates that vulnerability rarely emerges through a single catastrophic event. It develops through cascading pressure across interconnected systems. High-intensity conflict, cyber disruption, contested supply chains and climate-driven infrastructure shocks each expose different weaknesses, but the underlying pattern remains consistent: systems fail fastest where redundancy is absent and where dependencies remain poorly understood.

This report makes eight findings. Significantly, it identifies that Australia lacks a practical framework for assessing northern defence as a system rather than as a series of individual investments. Existing approaches remain fragmented across portfolios, agencies and sectors. Infrastructure expansion alone doesn't guarantee operational endurance if fuel, logistics, workforce and sustainment constraints remain unresolved. Redundancy is the decisive variable in contested conditions. Systems that maintain alternative pathways, backup capacity and distributed support mechanisms absorb disruption more effectively and recover more quickly. While prevention is ideal, preparedness requires institutional integration well beyond the Defence organisation. Northern resilience depends on coordination across federal, state and territory governments, industry, infrastructure operators and allied partners.

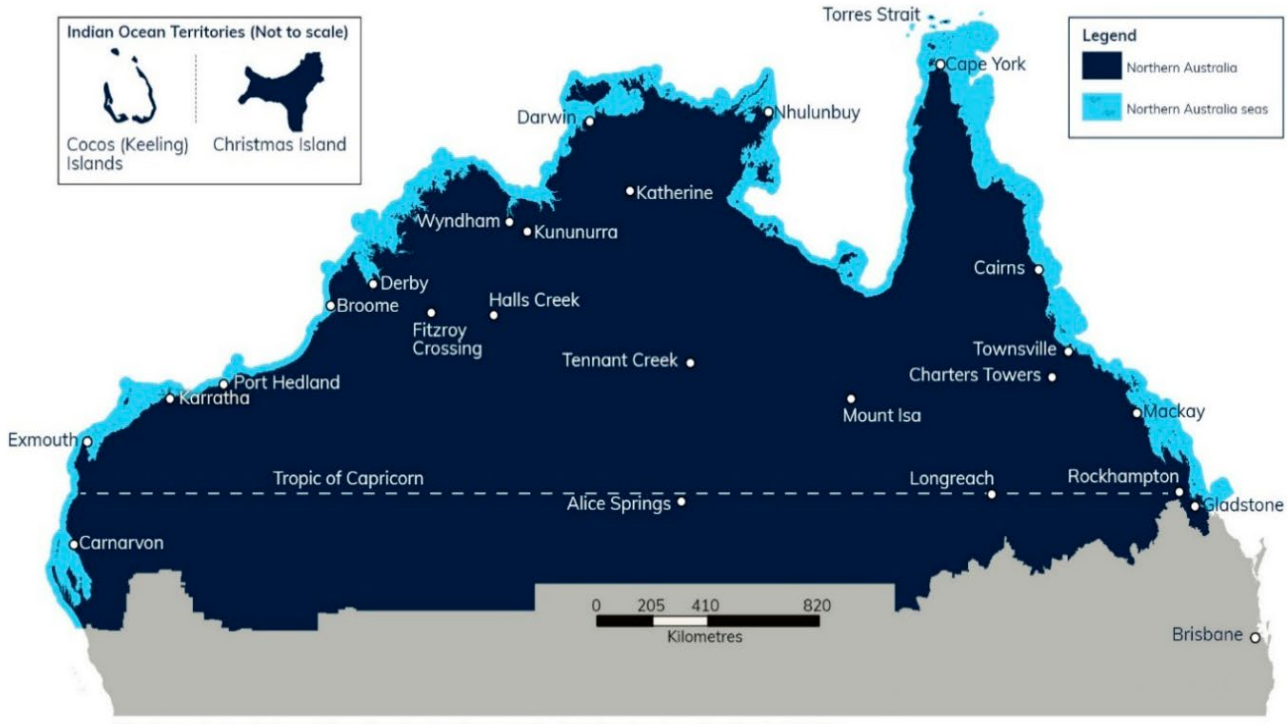
This report recommends a structured pilot to test and refine the PRR methodology across a limited number of high-value domains before broader institutional adoption. Defence's Resilience Division is the strongest candidate for initial custodianship, given its cross-portfolio responsibilities and access to relevant planning processes.

There's no doubt that Northern Australia is central to Australia's defence strategy. The remaining question is whether the systems that underpin northern defence can sustain the burden that strategy now places upon them.

Key findings and recommendations

1. *Australia lacks a system-level preparedness framework for northern defence.* Current assessment approaches measure projects, spending and infrastructure delivery. They don't measure whether the broader northern defence system can sustain operations under contested conditions. No existing framework integrates defence posture, civilian infrastructure, logistics, workforce and sustainment into a single operational assessment model.
2. *Northern defence operates as an interconnected system.* Fuel, logistics, infrastructure, energy, workforce, digital networks and industrial capacity depend on one another. Failure in one domain rapidly degrades others. Under compound stress, disruption cascades across the system faster than traditional planning frameworks can capture.
3. *Redundancy determines whether the system holds under pressure.* Scenario testing shows that systems absorb disruption only where alternative pathways, backup capacity and surge mechanisms already exist. Where redundancy is weak or absent, cascading failure becomes likely. Resilience can't exist without deliberate investment in redundancy.
4. *Current investment approaches risk reinforcing visible capability rather than operational endurance.* Infrastructure growth alone doesn't guarantee preparedness. Expanding ports, runways or facilities delivers limited operational effect if fuel distribution, logistics throughput, sustainment capacity or workforce depth remain constrained. The central investment question isn't what expands capacity, but what unlocks system performance.
5. *Workforce and sustainment constraints remain structural vulnerabilities.* Northern defence depends on specialised labour, industrial support, logistics coordination and civilian enabling systems that can't be surged easily during crisis conditions. Workforce fragility represents one of the most persistent constraints across all domains.
6. *Preparedness depends on integration across government and industry.* Northern resilience can't be delivered by the Defence organisation alone. Critical dependencies sit across state and territory governments, infrastructure operators, commercial logistics providers, energy systems and industry supply chains. Fragmented planning reduces overall system effectiveness.
7. *The PRR Scorecard provides a practical decision-support framework.* The PRR Scorecard gives decision-makers a structured method to identify vulnerabilities, test assumptions, sequence investment and assess operational risk across the northern defence system as a whole.
8. *A structured pilot should precede broader institutional adoption.* A limited pilot across two or three high-priority domains would validate the methodology, identify data gaps and refine governance arrangements before wider implementation. Defence's Resilience Division is the strongest candidate to assume initial custodianship of the framework.

Figure 1: Northern Australia



"Northern Australia" as defined by the *Northern Australia Infrastructure Facility Act 2016*.

Source: Office of Northern Australia.

Introduction

Northern Australia now sits at the centre of Australia's defence posture. It will generate, sustain and project military power if deterrence fails and Australia must execute a strategy of denial. The challenge is whether the systems that underpin northern defence can withstand disruption, absorb shock and sustain operations under pressure.

Over the past decade, Australian defence policy has steadily repositioned the north from a remote support area to a primary operating environment. The 2012 Australian Defence Force Posture Review identified Northern Australia as strategically decisive within Australia's evolving defence geography. The 2014 United States Force Posture Agreement deepened that shift through rotational US force presence, expanded air cooperation, logistics prepositioning and infrastructure investment. The 2023 Defence Strategic Review (DSR) then recast the north as fundamental to deterrence by denial, long-range strike and operational survivability. The 2024 and 2026 National Defence Strategy (NDS) documents institutionalised that transition by embedding national defence, integrated deterrence and system resilience into defence planning (Figure 2).

Figure 2: 2026 National Defence Strategy architecture

Source: 2026 National Defence Strategy.

Taken together, those changes impose a different burden on northern Australia. Defence no longer depends solely on bases, platforms or individual projects. It depends on the performance of an interconnected operating system that includes fuel, energy, logistics, ports, roads, digital networks, workforce depth, sustainment capacity and civilian infrastructure. That system stretches across Darwin, Tindal, Curtin, Learmonth, regional ports, fuel distribution corridors and remote logistics networks operating across some of the most dispersed and infrastructure-constrained environments in the Indo-Pacific. Failure in one domain now carries consequences across all others.

Current assessment approaches struggle to measure that reality. Governments can track expenditure, infrastructure delivery and force posture activity, but those indicators don't reveal whether the broader system can continue functioning once stressed. They don't show how quickly capability degrades, where bottlenecks emerge, or which dependencies are most likely to fail first under compound disruptions.

Current frameworks can measure runway upgrades at Tindal or infrastructure expansion in Darwin. They struggle to assess whether the broader logistics, fuel and sustainment system could maintain operational tempo once disruption spreads across the region simultaneously.

As strategic weight shifts north, the gap between investment visibility and operational readiness becomes more consequential.

Hardening northern defence therefore requires more than additional projects or larger budgets. It requires a disciplined way to assess whether the enabling ecosystem can sustain operational effect under contested conditions. That challenge sits at the centre of this report.

The Preparedness, Resilience and Redundancy (PRR) Scorecard responds to that problem. It provides a structured framework for assessing northern defence as a connected system rather than as a collection of individual capabilities. The framework focuses on performance under stress: how systems absorb disruption, maintain operational function and recover when degraded. Its purpose isn't to rank organisations or generate another reporting mechanism. Its purpose is to improve decision-making by identifying where the system is robust, where it's fragile and where investment will deliver the greatest operational effect.

This report argues that northern defence preparedness is ultimately a system-performance challenge. Strategic intent alone won't deliver deterrence credibility. The north must function as an integrated operational ecosystem capable of sustaining force generation, logistics, recovery and endurance under pressure. Whether Australia can achieve that outcome will shape the credibility of its broader defence strategy.

The assessment gap

Strategic ambition has outrun practical assessment. Users can point to investment under the Integrated Investment Program (IIP) as evidence of progress, but those measures show motion; they don't show readiness. They don't reveal whether northern defence can absorb disruption and continue to generate combat power under contested conditions.

Project counts and spending figures can't answer the questions that matter most: how fuel networks, logistics corridors, data links, workforce depth and sustainment capacity will perform under pressure, and what happens when multiple elements fail simultaneously. Without a disciplined framework to assess where the system is robust, where it's fragile and where it's likely to fail, investment decisions risk reinforcing visible capability at the expense of structural resilience.

The 2026 NDS frames the north as an integrated operating system, but the analytical tools used to assess it haven't kept pace with that framing. There's currently no structured, system-level method for evaluating preparedness, resilience and redundancy across northern defence as a coherent whole.

From concept to application

Current investment frameworks struggle to identify which constraints actually limit operational endurance. Runway expansion, fuel storage, logistics throughput and workforce depth don't contribute equally to operational effect. Some investments expand visible capacity. Others determine whether the system continues functioning once disruption begins. The PRR Scorecard is designed to expose those distinctions.

For example, a relatively small investment in fuel-distribution redundancy may deliver greater operational effect than a major expansion of runway capacity if fuel throughput remains the binding constraint on sortie generation.

Adopted at scale, the PRR Scorecard would move northern defence analysis beyond individual projects and towards an integrated operating ecosystem capable of sustaining a strategy of denial, not in intent, but in practice.

> The scorecard shifts the question from *'What have we built?'* to *'What can the system actually do when parts of it are degraded or fail?'*

Theoretical foundations

System-of-systems thinking

Northern defence isn't meant to function as a collection of discrete assets, but as a connected ecosystem in which air power generation, maritime sustainment, energy supply, ports, roads, rail, fuel storage, digital networks, workforce capacity and civilian infrastructure interact continuously and interdependently. In a contested environment, adversaries don't need to defeat the force directly; they need only to fracture the system that sustains it.

The 2026 NDS directs defence's domestic force posture to deliver a logistically network and resilient set of bases, predominantly across northern Australia to enhance force projection and improve defence's ability to recover from an attack.[1] System-of-systems thinking provides the conceptual framework that matches this reality.

As outlined in Figure 3 and Figure 4, John Holland's work on complex adaptive systems describes systems composed of multiple interacting elements that adapt, respond, and produce outcomes that can't be understood by examining any single component in isolation.[2] Elinor Ostrom later argued for diagnostic approaches that treat complex, multilevel systems as interconnected rather than reducible to a single variable or institution.[3] Defence functions as a system of systems, in which interdependent networks collectively determine operational resilience. In northern Australia, this reframes the central question: not whether any individual base, airfield, port or enabling infrastructure is sufficient in isolation, but whether those elements function together as a coherent whole. Bases depend on power, fuel, water, roads, ports, communications, housing and skilled labour, and failure in one domain degrades performance across all others.

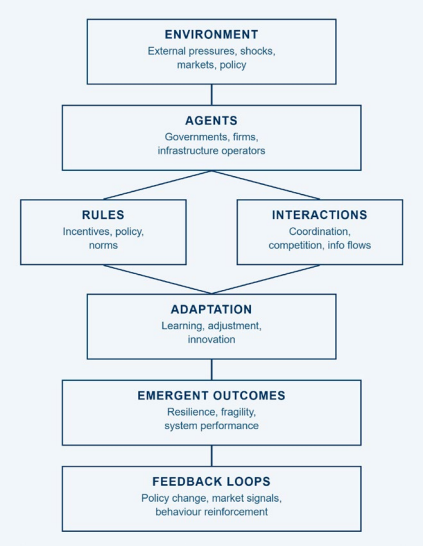
The workforce dimensions of that dependency—housing affordability, labour availability and community sustainability—are load-bearing elements of the system, not peripheral considerations; they're examined in detail in subsequent sections.

The northern defence network must therefore be assessed on whether it can continue to operate when stress cascades simultaneously across all those domains. Australia's northern defence strategy will succeed or fail in that chain of interdependence.

Charles Perrow's theory of normal accidents sharpens the point.[4] Perrow argued that tightly coupled, complex systems generate failures that are often unavoidable: interactions occur too quickly and too opaquely for operators to intervene once disruption begins. In such systems, failures don't remain local—they propagate. For a system of this complexity, that propagation creates numerous decision windows of varying duration, many of which may narrow or close before commanders can act.[5]

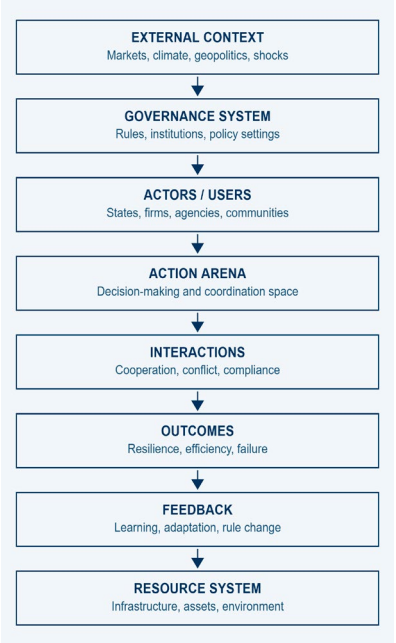
The Indo-Pacific itself offers an instructive precedent. During World War II, supply disruption, distance, weak advance-base infrastructure and competition for shipping and resources

Figure 3: Complex adaptive systems



Source: JH Holland, 'Complex adaptive systems', *Daedalus*,1992, 21(1):17–30, online.

Figure 4: Diagnostic framework overview



Source: E Ostrom, 'A diagnostic approach for going beyond panaceas', *Proceedings of the National Academy of Sciences*, 2007,104(39):15181–15187, online.

repeatedly constrained Allied operations across the Pacific, producing shortfalls in fuel, stores, maintenance and sustainment capacity that degraded operational tempo across entire theatres.[6] That structural vulnerability hasn't been resolved; it has deepened. The acknowledged fragility of contemporary US fuel supply chains across the Indo-Pacific, where forward stocks are limited, distances are vast and maritime resupply routes are increasingly contested, reflects the same systemic logic in a more complex and compressed operational environment.[7]

For northern Australia, cascading failure creates numerous decision windows of varying duration.[8] Those windows are determined by the speed of the cascade, the visibility of the initiating failure, and whether response capacity has been pre-positioned close enough to matter. When windows close (as Perrow's framework suggests they frequently do) before operators can intervene, failure becomes self-reinforcing and the options available contract sharply.[9]

That logic is reinforced by the US Department of Defense Joint Concept for Integrated Campaigning (JCIC),[10] which argues that enduring strategic outcomes depend on the alignment of military and non-military systems across multiple domains and over extended periods. The JCIC rejects the notion that military capability can be assessed independently of its supporting environment, instead emphasising the importance of logistics, infrastructure, workforce, access, industry and governance as interconnected enablers of operational effectiveness. From that perspective, preparedness, resilience and redundancy aren't simply desirable characteristics of individual assets; they're system-level attributes that determine whether the broader defence network can absorb disruption, adapt under stress and continue generating military effect.

The PRR Scorecard therefore functions as a diagnostic framework for assessing the readiness of the northern defence ecosystem as an integrated campaign system, rather than as a collection of stand-alone facilities or capabilities.

Fuel case study

Fuel sits at the base of operational endurance. It powers logistics. Logistics moves munitions. Munitions sustain force generation. Every stage in that chain depends on digital systems coordinating movement, distribution and command across vast and dispersed operating environments (Figure 5).

Disrupt one node and pressure propagates quickly across the system. A fuel outage doesn't merely delay resupply. It constrains logistics throughput, slows maintenance cycles, reduces mobility and weakens command continuity. As disruption compounds, operational tempo contracts, responsiveness degrades and surge capacity erodes. The result isn't simply reduced efficiency, but a declining ability to generate and sustain combat power over time.

Network resilience research reaches the same conclusion from a different direction. Studies of interdependent infrastructure networks show that power, communications, transport and other essential services don't merely coexist; they rely on one another in ways that can trigger cascading failure when one layer degrades.[11]

Critically, this isn't a linear relationship between cause and effect. It's a structural property of tightly coupled systems: small disturbances can produce disproportionate, system-wide collapse precisely because dependencies are opaque until they're stressed, and because the failure of one network removes the support on which adjacent networks rely.

'Cascading failure' describes that dynamic precisely. Cascading failures are a common phenomenon in complex networked systems in which the failure of a small number of nodes may trigger a process of sequential failure, eventually making the whole system break down.[12]

Studies of dependent and interdependent infrastructure networks have shown that resilience assessment must account for those cross-network dependencies.[13] At the same time, later work on interdependent networks demonstrates that small disturbances can trigger disproportionate, system-wide collapse.

Cascading failure is a useful way to understand how interdependence shapes operational resilience. In a system of systems such as northern defence, critical functions such as fuel, logistics, munitions movement and force generation don't operate independently. They're tightly coupled through physical infrastructure and coordinated through digital networks. When one node is disrupted, the impact doesn't remain contained; it spreads across connected systems, compounding over time.

Research on infrastructure interdependence also shows that redundancy, backup arrangements and adaptive practices can reduce cascade severity, but only if planners identify dependencies early and design for them deliberately.[14]

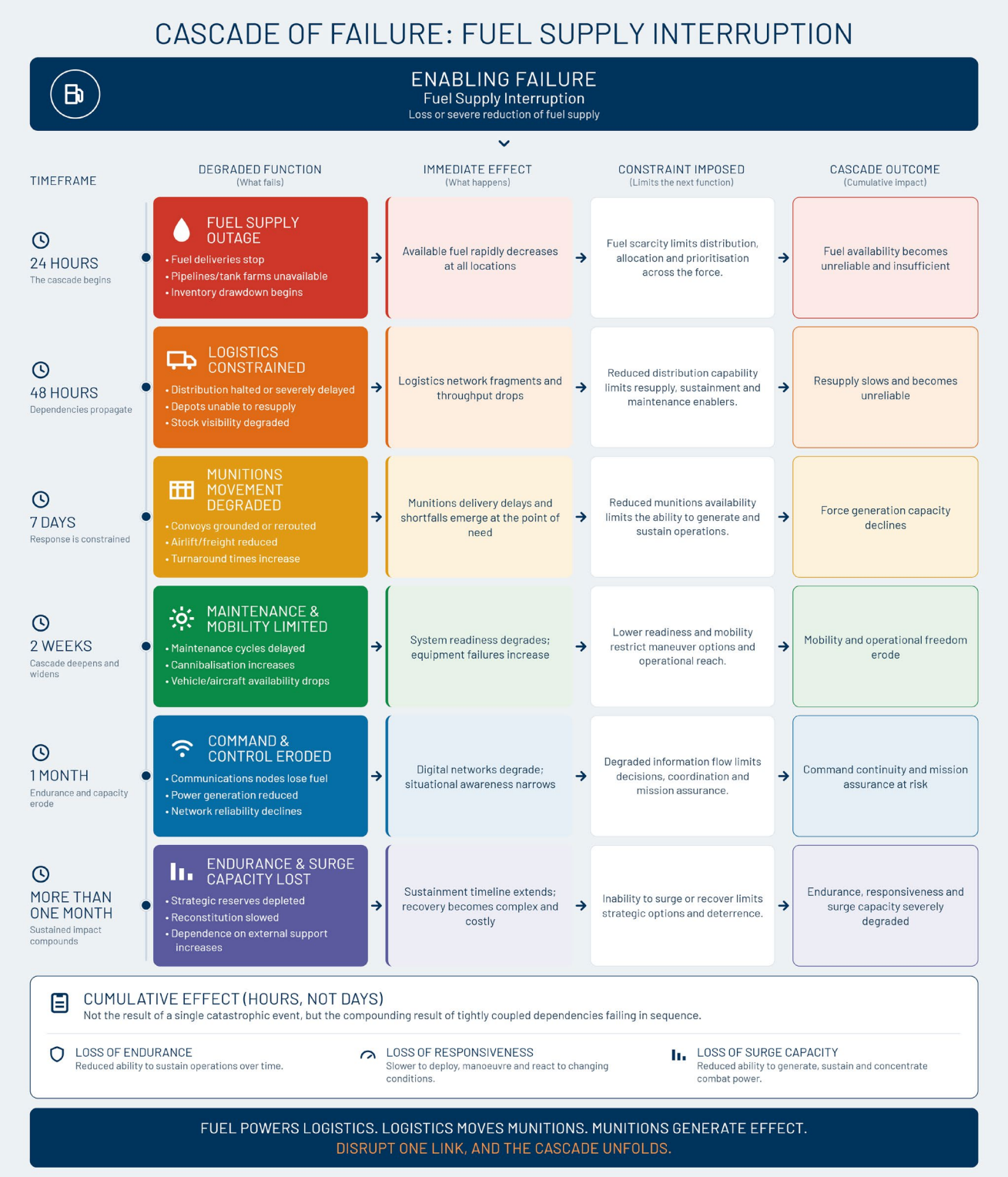
In comparable austere environments, that's meant pre-positioned fuel reserves, hardened communications nodes with independent power sources, and pre-agreed degraded-mode operating procedures that allow functions to continue when digital coordination fails.

For northern Australia, where infrastructure density is low, distances are large and repair and resupply timelines are extended, the margin for unplanned redundancy is narrow. Whether equivalent design discipline has been applied to Australia's northern defence network is a question this report returns to in its assessment of capability gaps. Dependencies must be mapped. Resilience must be engineered, not assumed.

Power case study

A power outage at a northern defence base illustrates how quickly disruption spreads across the broader operating system (Figure 6). Initial loss of grid power forces facilities onto backup generation, immediately narrowing redundancy margins and reducing operational flexibility. As power availability contracts, pressure emerges across fuel systems, communications networks, maintenance functions and security infrastructure simultaneously.

Figure 5: An example of the impact of a fuel supply outage



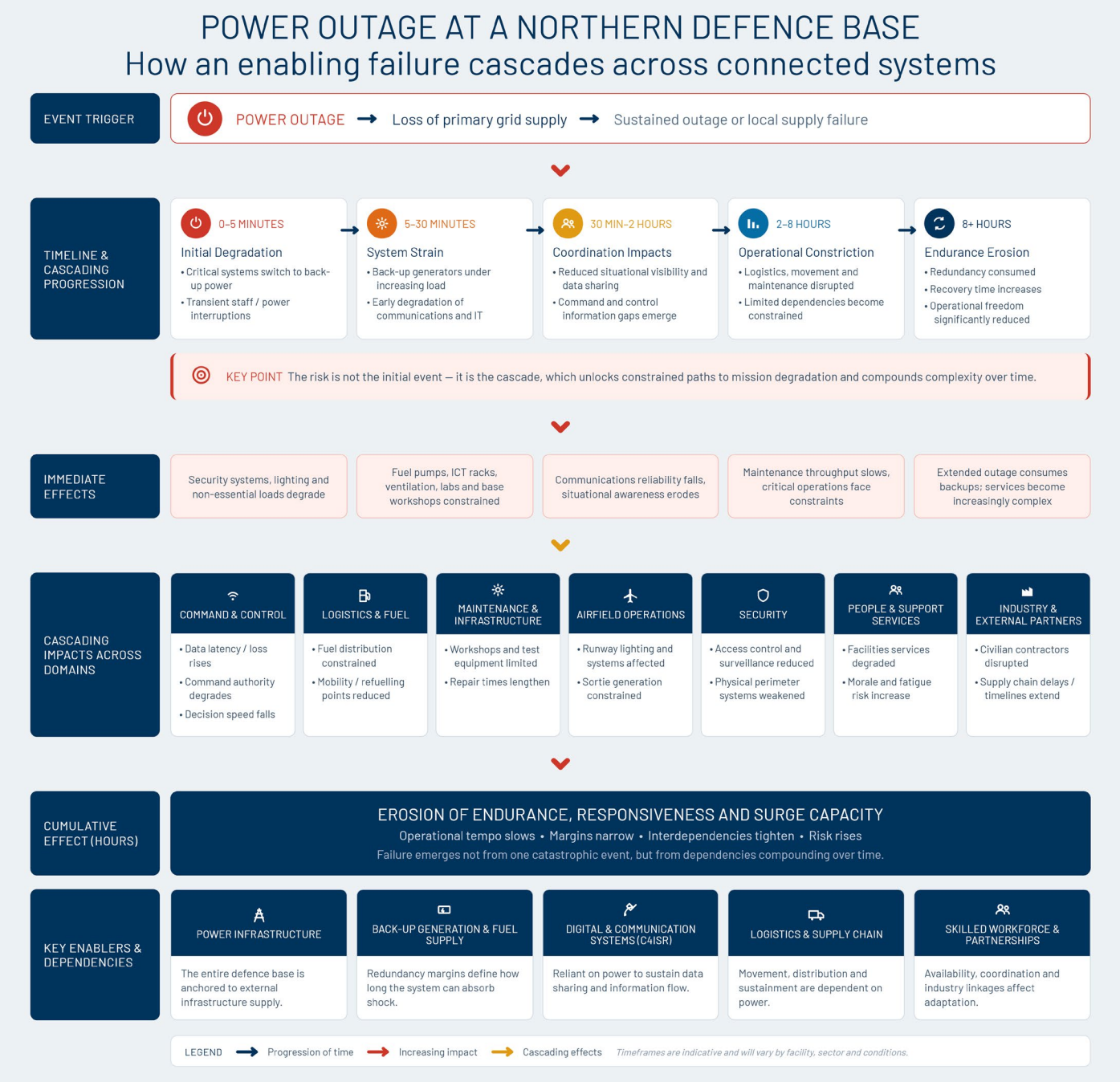
Source: ASPI.

In locations such as Darwin, Tindal and remote Northern Territory operating sites, restoration timelines may depend on long logistics chains, contractor availability and transport access across vulnerable road networks already operating with limited redundancy.

Digital systems begin to degrade first. Data latency increases. Network reliability weakens. Communications become less stable across dispersed operating locations. As coordination slows, commanders lose visibility over logistics movements, maintenance priorities and force readiness. What begins as an energy disruption rapidly becomes a command-and-control problem.

The effects then compound across the base ecosystem. Fuel-distribution systems become constrained. Maintenance throughput slows as workshops, cooling systems and specialist

Figure 6: An example of cascading failure at a northern base



Source: ASPI.

equipment lose reliable power. Airfield operations face increasing pressure as lighting, communications and support systems degrade. Civilian contractors and external service providers become harder to coordinate precisely when demand for repair and sustainment rises.

The critical issue isn't the initial outage itself. Northern defence infrastructure contains some redundancy and backup generation capacity. The strategic risk emerges when disruption persists long enough to consume those buffers faster than they can be restored. As redundancy narrows, recovery timelines lengthen and operational flexibility contracts.

The cumulative effect is progressive erosion of endurance, responsiveness and sustainment capacity across the broader northern defence system. Failure doesn't emerge through a single catastrophic event. It develops through interconnected systems degrading in sequence faster than operators can stabilise them.

Vulnerability and resilience theory

Vulnerability and resilience theory offers the second pillar for the PRR Scorecard.

System-of-systems thinking explains why disruption can spread. Vulnerability and resilience theory helps to judge how well a system can withstand that disruption, recover from it and adapt under pressure. Globally, critical infrastructure frameworks have moved steadily in that direction.

The US National Infrastructure Protection Plan treats security and resilience as linked outcomes. It defines resilience as the ability to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions.[15]

The Organisation for Economic Co-operation and Development (OECD) takes a similarly broad approach, treating resilience as a governance challenge that must run across the full infrastructure life cycle rather than sit at the margins of emergency planning.[16]

The UK's National Risk Register adds a public-facing model that assesses acute national risks and encourages institutions, businesses and communities to build preparedness before a crisis strikes.[17]

Those frameworks push policy away from narrow asset protection and towards continuity of function. Northern defence requires a shift in the question being asked. The survivability of individual assets is necessary but insufficient. The measure that matters most is whether northern defence, as a whole, can continue to generate, move, sustain and recover force under stress.

This broader lens aligns with the baseline requirements for national resilience of the North Atlantic Treaty Organization (NATO), which focus on continuity of government, energy, civil communications, transport systems and support to military operations.[18]

The Baltic states have embedded a similar logic into whole-of-society defence approaches. Estonia's comprehensive defence model links military defence, civil support, essential services and societal readiness. In contrast, Lithuania's security strategy and defence policy emphasise total defence, critical infrastructure resilience and crisis readiness across state institutions and society.[19]

Israeli practice reinforces the value of hardening and continuity planning. The National Emergency Management Authority under Israel's Ministry of Defense coordinates home-front emergency preparation. It aims to maintain national resilience and functional continuity during crises. Israel's longstanding emphasis on protected spaces, emergency management and infrastructure reinforcement shows that hardening matters only when it supports the continuity of operations and civilian endurance together.[20]

Precedents

Governments don't approach resilience as an abstract concept. Many have developed structured frameworks, scorecards and assessment tools to measure preparedness, prioritise investment and guide policy. Those models provide useful precedents for the PRR Scorecard. They also reveal a consistent limitation. Most frameworks assess resilience within sectors. Very few integrate defence posture with civilian infrastructure in a single operating model.

The US Federal Emergency Management Agency (FEMA) has developed community-level resilience assessment tools that allow jurisdictions to evaluate preparedness across infrastructure, social systems and emergency management capacity. FEMA's National Preparedness System links risk assessment, capability targets and evaluation to support continuous improvement across federal, state and local levels.[21] Those tools provide structured ways to identify gaps and prioritise investment. Still, they remain oriented towards disaster response rather than sustained military operations.

NATO's baseline requirements for Resilience, Civil Preparedness and Article 3 offer a more security-focused model.[22] Those benchmarks require member states to ensure continuity of government, resilient energy supplies, secure communications, robust transport systems and the capacity to support military operations. NATO's framework recognises that military effectiveness depends on civilian infrastructure. However, it sets minimum standards rather than providing a diagnostic tool for investment sequencing at the national or regional level.

The UK's National Infrastructure Commission[23] and National Risk Register[24] take a complementary approach by assessing long-term infrastructure resilience across energy, transport, water and digital systems, and the register provides a public assessment of national-level threats and system vulnerabilities. Those frameworks emphasise cross-sector dependency and long-term planning. Yet, they don't explicitly integrate defence posture or operational sustainment requirements.

Finland's Total Defence Model places particular emphasis on security of supply and the resilience of critical national systems.[25] Through the National Emergency Supply Agency, Finland coordinates government, industry and infrastructure operators to identify vulnerabilities, maintain strategic reserves and strengthen preparedness across energy, transport, communications, logistics and other essential sectors. The agency employs structured assessment and planning mechanisms to ensure continuity during crises and conflict, providing a practical example of how resilience can be measured and managed across an interconnected system. That approach demonstrates the value of systematic preparedness assessment, although its focus remains national in scope rather than on a specific operational theatre.

Sweden's Total Defence Model integrates civil preparedness, crisis management and military readiness through the Swedish Civil Contingencies Agency.[26] The agency coordinates preparedness activities across government, industry, local authorities and civil society, using risk assessments, resilience planning and regular exercises to strengthen national readiness. By recognising that disruptions in one sector can rapidly affect others, the Swedish model reinforces the importance of understanding infrastructure as an interconnected system. That approach highlights the role of coordinated governance and continuous assessment in building resilience, while remaining focused on whole-of-nation preparedness rather than the regional infrastructure systems of the type that support defence operations in northern Australia.

Singapore's Total Defence Framework takes a whole-of-society approach by integrating the military, civil, economic, social, digital and psychological dimensions of resilience.[27] The framework uses structured indicators and public engagement to measure readiness

and reinforce national cohesion. That model demonstrates how resilience can extend beyond infrastructure into societal capacity. Still, it remains focused on national mobilisation rather than regional system design.

Japan's National Resilience Basic Plan provides another instructive example.[28] Japan has embedded resilience planning into national policy following major natural disasters. The plan identifies critical infrastructure vulnerabilities, sets investment priorities and promotes redundancy across transport, energy and communications systems. The framework emphasises continuity and rapid recovery, but it focuses primarily on disaster resilience rather than contested operational environments.

Collectively, those frameworks demonstrate that preparedness and resilience are increasingly assessed through structured, repeatable mechanisms that extend beyond military capability alone. While each model reflects its own strategic context, all seek to identify vulnerabilities, prioritise investment and strengthen the capacity of critical systems to withstand disruption. The PRR Scorecard draws on those international approaches but adapts them to the unique requirements of northern Australia, focusing on the regional infrastructure systems that enable defence posture, mobilisation and sustained operations.

Australia

Australia has also moved in that direction through the *Security of Critical Infrastructure Act 2018* (SOCI Act) and associated risk-management programs. The SOCI framework requires operators of critical infrastructure assets to identify hazards, assess vulnerabilities and implement risk-management plans across sectors such as energy, water, transport and communications.[29] The SOCI framework strengthens national resilience but remains sector-based and doesn't integrate defence operational requirements.

A clear pattern emerges from these frameworks. Governments recognise the need to measure resilience and have developed increasingly sophisticated tools to assess risk, identify gaps and guide investment. Yet a structural limitation persists across almost every model.

Sector-based frameworks, however comprehensive, don't integrate defence posture and operational sustainment requirements. Security-focused frameworks, however rigorous, set minimum viable standards rather than providing diagnostic tools capable of sequencing investment across an interdependent regional system. Nearly all existing frameworks are oriented towards disruption response or national mobilisation, not towards the sustained generation of combat power in a contested operating environment. The gap isn't intentional but is still architectural.

Northern defence sits precisely at the intersection those frameworks don't reach. Its effectiveness depends not on any single sector performing well in isolation but as an ecosystem functioning together under pressure. That isn't a disaster resilience problem or a standards compliance problem. It's a system performance problem—one that requires a tool designed specifically to assess whether the ecosystem can continue to generate, move, sustain and recover force when parts of it are degraded or denied.

The PRR Scorecard is designed to help us understand that gap. It builds on the structured assessment logic evident in existing frameworks while resolving the limitation they share: the absence of a cross-sector diagnostic tool calibrated to operational sustainment rather than disaster response.

By assessing preparedness, resilience and redundancy across northern defence as a connected system, the PRR Scorecard provides a disciplined assessment methodology to identify where the system is robust, where it's brittle and where investment will deliver the greatest contribution to enduring strategic effect.

Building the PRR framework

Design principles

A credible scorecard requires disciplined design. Northern defence operates within a complex and interdependent operating environment in which false precision can distort judgement rather than improve it. The PRR Scorecard therefore uses a structured qualitative methodology that combines operational insight, practitioner experience and contextual assessment to evaluate system performance consistently across domains.

The framework links vulnerability directly to operational effect. Identifying gaps has limited value unless their consequences are understood in practical terms. A constraint in munitions handling limits sortie generation. Weak energy redundancy constrains sustainment, recovery and operational endurance. The critical question isn't whether a vulnerability exists, but what that vulnerability prevents the system from doing under stress.

Preparedness also changes over time. Infrastructure degrades, demand patterns shift and threats evolve. The PRR Scorecard must therefore support continuous reassessment, allowing assumptions, priorities and investment decisions to adjust as operating conditions change.

Accessibility is equally important. A framework that can't be shared across governments, industry and key partners won't shape decisions effectively. The PRR Scorecard should minimise unnecessary classification barriers while still reflecting operational reality. Its purpose is to align decision-making across the broader preparedness system, not to restrict participation within it.

Table 1: The PRR scorecard framework

PRR Scorecard Framework		
Tier 1: Immediate operational viability **Determines whether denial holds at the point of contact**		
Force posture and forward presence ↓ Project, position and persist combat power forward in key theatres.	**Logistics and sustainment** ↓ Deliver, distribute and sustain operations in contested and degraded environments.	**Fuel and energy security** ↓ Assured access to fuel and energy to enable operations and sustain force projection.
Tier 2: System sustainment and endurance **Determines whether denial can be sustained over time**		
Strategic infrastructure and estate ↓ Bases, ports, airfields and enabling infrastructure that underpin operational reach, survivability and recovery.	**National support base (civil–military integration)** ↓ Integration of the Defence organisation with national and commercial systems that provide critical goods, services and logistics.	**Industrial base and regeneration capacity** ↓ Ability to produce, repair, replace and scale capability under sustained demand.
Tier 3: Integration, decision and scaling advantage **Determines how effectively the system adapts, integrates and scales under pressure**		
Digital, decision and command systems ↓ Data, communications, power and decision-making architectures that enable coordinated, timely and distributed operations.	**Integration with allies and partners** ↓ Interoperability, burden-sharing and access to allied capability, infrastructure and supply chains.	**Workforce and human capital** ↓ Capacity to generate, sustain and adapt a skilled workforce across Defence, industry and supporting systems.

Core domains

The PRR Scorecard assesses northern defence preparedness, resilience and redundancy across nine interdependent domains organised into three tiers (Table 1). Each tier reflects a distinct dimension of operational performance, and each domain is in a core question.

Tier 1: Immediate operational viability determines whether denial holds at the point of contact.

- *Force posture and forward presence* is the capacity to project, position and sustain combat power forward in key theatres. It determines whether northern bases can generate and sustain operational tempo under disruption such as runway redundancy, dispersed basing options, munitions-handling capacity and rapid repair capability. Without it, denial has no forward edge.
- *Logistics and sustainment* is the ability to deliver, distribute and sustain operations in contested and degraded environments. It determines whether supply chains remain functional when maritime access is disrupted, transport corridors are degraded or digital coordination is denied. Logistics is the connective tissue of the operating system—its failure compounds across all domains.
- *Fuel and energy security* is assured access to fuel and energy for sustained operations. It determines whether the system can function during prolonged supply disruption, including to storage depth, distribution resilience, grid stability and distributed generation capacity. Fuel underpins all domains; its loss rapidly generates cascading failures throughout the wider system and represents one of the most critical determinants of operational endurance.

Tier 2: System sustainment and endurance determines whether denial can be sustained over time.

- *Strategic infrastructure and estate* includes bases, ports, airfields and enabling systems that underpin operational reach, survivability and recovery. It determines whether the physical foundation can absorb damage, maintain functionality and sustain operations, not just support during short-duration activity.
- *The national support base* is the integration of the Defence organisation with national and commercial systems. It determines whether civilian supply chains and service networks can be mobilised under surge conditions, and whether that integration is pre-planned or improvised under stress.
- *Industrial base and regeneration capacity* is the ability to produce, repair, replace and scale under sustained demand. It determines whether combat power can be regenerated after attrition and includes maintenance throughput, battle damage repair, supplier depth and workforce capacity.

Tier 3: Integration, decision and scaling advantage determines how effectively the system adapts, integrates and scales under pressure.

- *Digital, decision and command systems* comprise the data, communications, power and decision-making architecture that enables coordinated operations. While assessed as a discrete domain, it also functions as a crosscutting dependency that

influences performance across all other domains. Disruption can rapidly degrade logistics, fuel distribution, force generation, infrastructure management and command functions, amplifying operational risk across the system.

- *Integration with allies and partners* is the extent to which interoperability and burden sharing translate into operational effect. It determines whether alliances deliver shared logistics, compatible systems and coordinated responses, rather than proximity without integration.
- *Workforce and human capital* is the capacity to generate, sustain and adapt a skilled workforce across Defence and industry. It determines whether the system can scale without extraordinary intervention. Workforce remains the most persistent and least substitutable constraint across all domains. Without sufficient skilled personnel, otherwise resilient infrastructure, logistics and industrial systems can't generate operational effect.

Scoring approach

Each domain is assessed across three pillars using a scale (Table 2).

Table 2: PPR pillars

Pillar 1: Preparedness	Pillar 2: Resilience	Pillar 3: Redundancy
Is the deliberate work undertaken in advance to enable rapid and effective response.	Is the ability to absorb shock and continue operating under stress.	Is the deliberate provision of alternative capacity or pathways so that failure in one element doesn't lead to system collapse.

The scale is diagnostic, not performative. Its purpose isn't to rank organisations or assign blame, but to identify where the system is robust, where it's developing and where it's most likely to fail under stress.

Scores must be supported by narrative evidence. A number without explanation obscures more than it reveals. The evidence requirement ensures that assessments reflect how systems perform under stress, not how they're designed to perform in steady state.

The value of the PRR Scorecard lies in patterns across domains. It reveals systemic vulnerability and investment priorities, rather than isolated strengths or weaknesses.

Scoring should be grounded in observable, domain-specific behaviours. For example, in fuel and energy security, maturity is reflected not just in plans, but in exercised systems, active redundancy and demonstrated continuity under disruption.

While all nine domains are essential to operational effectiveness, they don't contribute equally to system performance. Some domains function as foundations (such as fuel and energy security; workforce and human capital; and digital, decision and command systems), which, if deteriorated, would rapidly constrain multiple domains. Therefore, the purpose of the scorecard isn't merely to identify weak domains but to identify where those weaknesses are most likely to generate cascading effects across the wider system (Table 3).

Table 3: PRR scoring categories

Score	Maturity level	Description	Performance under stress
1	Fragile	Capability very weak or not in place	Likely to fail immediately under scenario conditions
2	Limited	Basic capability exists but fragile	Will fail under sustained or compound pressure
3	Functional	Performs adequately under peacetime conditions	Partial resilience under stress
4	Resilient	Robust under most stress conditions	Alternative pathways or backup systems operational
5	Adaptive / surge-ready	Maintains full capability under contested conditions	Redundant systems auto-activate

While the PRR maturity scores provide a snapshot of capability development, they don't fully capture operational risk. The three overlays presented in Table 4 (time to failure, time to recovery and external dependence) provide the analytical layer that translates maturity into operational consequence.

Together, they assess how quickly a domain may degrade under pressure, how difficult it may be to restore, and the extent to which continued performance relies on external physical and digital systems beyond Defence's direct control. In doing so, they reveal the pathways through which vulnerabilities propagate across the wider system and help to identify where localised disruptions might generate cascading operational effects.

The overlays therefore serve as the principal diagnostic mechanism within the framework, enabling assessors to distinguish between domains that are merely underdeveloped and those that represent critical operational vulnerabilities requiring priority attention.

Table 4: PRR scoring overlays

Time to failure	Time to recovery	External dependence
Captures how quickly a domain would degrade from normal operations to ineffective performance when subjected to disruption, degradation or sustained pressure. This reflects the domain's inherent robustness, available buffers, surge capacity and ability to continue operating despite the loss of key inputs or services. Shorter times to failure indicate greater vulnerability and a higher likelihood of cascading effects across the wider system.	Captures how long a domain would take to restore effective operational performance following disruption, damage or loss of capability. This reflects the availability of repair capacity, replacement resources, workforce skills, supply-chain access, recovery planning and alternative operating arrangements. Longer recovery periods indicate greater operational risk and reduced ability to sustain prolonged operations.	Captures the degree to which a domain relies on systems, services, networks or supply chains outside Defence's direct control. This includes civilian infrastructure, commercial providers, domestic and international supply chains, allied support arrangements and critical digital dependencies such as communication networks, satellite services, cloud platforms, data services and cyber-enabled systems. Higher dependence indicates greater exposure to disruption, delay or degradation during crisis or conflict.
Example scoring		
Immediate	Very slow	Critical exposure
Short term	Slow	High exposure
Moderate	Moderate	Moderate exposure
Sustained	Rapid	Limited exposure
Enduring	Immediate	Minimal exposure

Maturity assessment

Maturity is assessed in two stages to distinguish between how a domain is designed to perform and how it's likely to perform under stress.

First, each domain is assessed across the three pillars (preparedness, resilience and redundancy), using the five-point scale. Those aren't averaged but are read together as a profile to form a baseline maturity judgement. That reflects the internal balance of the domain and the extent to which it's coherently designed to anticipate, absorb and recover from disruption.

Second, that baseline assessment is adjusted by overlaying three additional factors: time to failure, time to recovery and dependence on external systems. Those overlays shift the assessment from design to operational reality, highlighting how quickly capability degrades, how long it takes to restore, and how exposed it is to disruption beyond sovereign control.

The result is a revised maturity judgement that reflects performance under contested conditions. The gap between baseline and adjusted maturity is analytically important, as it reveals where capability appears robust in design but is vulnerable in practice.

Managing subjectivity

Given the qualitative nature of the PRR Scorecard, subjectivity is unavoidable but manageable. A structured pilot phase should be used to calibrate scoring. In addition, a formal disagreement protocol should be adopted: where assessors differ by more than one point, both scores must be recorded alongside the rationale.

Disagreement is analytically valuable. It highlights gaps in data, divergent assumptions and differences between operational and policy perspectives. Capturing that variance strengthens the assessment rather than weakening it.

Scenario testing

The PRR framework is designed to assess system performance under pressure, not under normal operating conditions.

Scenario testing provides that discipline, forcing the analysis beyond static domain assessments to examine how vulnerability propagates, where cascading failure emerges and where redundancy proves insufficient to maintaining minimum viable capability.

Australia's northern defence faces three categories of compound disruption that don't arrive in isolation:

- *Climate and environmental events*, such as cyclones, flooding and extreme heat, can simultaneously affect logistics corridors, energy systems, workforce availability and infrastructure integrity. They aren't background conditions; they're operational variables that amplify stress across every domain they touch.
- *Cyber and digital disruption* removes the coordination layer on which all domains depend, multiplying its effect system-wide rather than containing it within a single domain.
- *Economic and supply-chain disruption* through import dependency, supplier failure or commercial withdrawal erodes the national support base and industrial regeneration capacity at precisely the moment demand increases.

The most demanding scenarios combine all three. A prolonged logistics disruption coinciding with a sustained cyber campaign would degrade digital coordination at the same time as physical supply chains are under stress, cascading across sustainment, force generation and command continuity. A major weather event during a period of military surge would introduce compound stress across infrastructure, workforce and logistics simultaneously, testing the integration of civilian and military systems at their limits.

Scenario testing anchors the PRR Scorecard in operational reality. It ensures that assessment remains focused on the question that matters: not whether the system performs under normal conditions, but whether it can absorb compound disruption and continue to generate, move, sustain and recover force under stress. Three scenarios illustrate how the scorecard can be applied.

Table 5: Scenario stress test panel

Stress test panel		
Scenario	**System stress**	**Likely failure points**
High-intensity conflict	Munitions, fuel, tempo	Force generation and logistics
Cyber and supply-chain disruption	Data, ports, coordination	Digital and logistics
Climate shock during operations	Energy, workforce, infrastructure	Energy and workforce

Scenario 1: High-intensity conflict

A high-intensity strike campaign places immediate pressure on fuel systems, logistics networks and force generation. Sustained sortie rates demand resilient fuel distribution, rapid munitions handling and reliable runway operations. Operational pressure is be likely to be concentrated around northern air and logistics hubs, including Darwin, Tindal, Curtin and Learmonth, where fuel throughput, runway repair and munitions handling become critical constraints on sustained sortie generation. Any disruption quickly constrains operational tempo.

Under pressure, vulnerability spreads rapidly across connected systems. Fuel disruption slows logistics. Logistics constraints reduce sustainment and sortie generation. In northern Australia, that pressure concentrates quickly along a small number of critical corridors and nodes. Fuel moving through Darwin, Tindal and the Stuart Highway network underpins much of the region's operational mobility and sustainment capacity. Disruption at any point in that chain rapidly affects force generation across dispersed operating locations. Redundancy in runway repair, fuel storage and distribution becomes decisive in determining whether operations can continue at scale. The challenge is magnified by distance. Sustainment pathways across northern Australia rely heavily on a limited number of ports, highways and fuel distribution corridors vulnerable to disruption or overload during sustained operations.

This scenario highlights the importance of investment in fuel resilience, munitions infrastructure and rapid repair capability to sustain operational endurance under contested conditions.

Scenario 2: Cyber and supply-chain disruption

A prolonged cyber campaign combined with supply-chain disruption places simultaneous pressure on logistics and digital coordination systems. Ports operate below capacity, freight networks slow and inventory visibility degrades. Delays at Darwin Port and East Arm rapidly affect fuel movement, sustainment sequencing and regional logistics coordination across northern Australia, particularly where remote operating locations depend on tightly timed resupply windows. As communications reliability weakens, decision-makers lose visibility over movements, prioritisation and sustainment.

The disruption compounds progressively rather than through immediate collapse. Reduced digital coordination amplifies logistics friction, which then degrades sustainment, force readiness and operational responsiveness across the broader system. In the Northern Territory operating environment, where distance already constrains transport flexibility, even minor disruption to routing, freight visibility or fuel coordination can generate disproportionate operational delays.

This scenario reinforces the importance of digital resilience, protected communications, diversified supply pathways and continuity planning across critical logistics networks.

Scenario 3: Climate shock during operations

A major cyclone or flood during a period of elevated operational demand places simultaneous pressure on infrastructure, logistics, energy systems and workforce availability. Ports close, transport corridors degrade and fuel distribution becomes constrained, while civilian recovery requirements compete directly with military sustainment needs. Flooding across the Stuart Highway corridor or cyclone disruption around Darwin and Katherine would place immediate pressure on fuel movement, sustainment access and workforce mobility across the broader northern operating environment.

This scenario highlights the shared dependence that civilian and military systems have on the same infrastructure, workforce and logistics networks. Defence, industry and civilian recovery operations would compete simultaneously for fuel, transport assets, repair capacity and skilled labour across a region already operating with limited surge depth. As disruption spreads, redundancy narrows and recovery timelines extend, particularly where systems rely on centralised infrastructure or limited alternative pathways.

This scenario demonstrates the importance of climate-hardened infrastructure, distributed energy systems, workforce continuity planning and redundant transport and sustainment networks.

Cross-scenario insights

Across all three scenarios, a consistent pattern emerges. Vulnerability rarely exists within a single domain. It develops through interaction between interconnected systems under pressure. Functions that appear resilient in isolation degrade quickly once disruption spreads across fuel, logistics, infrastructure, workforce and digital networks simultaneously.

The scenarios also demonstrate that redundancy is the decisive variable in determining whether the system absorbs disruption or begins to fail. Where alternative pathways, backup systems and surge capacity exist, operational pressure can be managed and recovery accelerated. Where they don't, cascading failure becomes increasingly difficult to contain.

The PRR Scorecard provides a structured framework for identifying those pressure points before they're exposed under real operational conditions. It shifts assessment away from static infrastructure and capability measures towards system performance under stress.

Scenario testing gives the framework operational relevance. It moves analysis beyond whether capability exists on paper and towards whether the broader northern defence system can continue to generate, sustain and recover operational effect during prolonged disruption.

Applying the PRR Scorecard

Northern defence investment doesn't fail through lack of activity. It fails when visible infrastructure expansion outpaces the enabling systems needed to sustain operations under pressure. The PRR Scorecard is designed to inform real investment and planning decisions, not sit beside them as another reporting framework. Its purpose is to help governments and industry understand which investments strengthen operational performance across the northern defence system and which simply add visible capacity without resolving underlying constraints.

Its most immediate value sits in investment sequencing. Not every project delivers the same operational effect. Expanding a runway delivers limited additional combat power if fuel distribution, munitions handling and logistics throughput remain constrained. In that case, the binding constraint isn't the runway; it's the enabling systems that allow aircraft to generate and sustain sorties.

Expanding ports, airfields or fuel storage doesn't automatically improve operational readiness. In many cases the constraint sits elsewhere: logistics throughput, maintenance capacity, workforce availability or energy distribution. The PRR Scorecard makes those trade-offs visible by shifting the investment question from 'What increases capacity?' to 'What improves system performance under pressure?'

The framework also exposes where interdependencies create operational risk. Existing frameworks such as the SOCI regime assess sector-level resilience. The critical question isn't what expands infrastructure capacity, but what allows the system to continue generating operational effect once disruption begins.

Its purpose isn't to centralise regional development around defence. Its purpose is to ensure that defence investment, infrastructure planning and economic resilience reinforce one another rather than develop separately and create new vulnerabilities in the process.

The core challenge

Current preparedness models measure inputs more effectively than they measure system performance. Governments can point to runway upgrades, fuel projects and infrastructure spending. Far fewer can explain how those systems would perform once fuel disruption, cyber degradation or logistics failure begin interacting simultaneously. The PRR Scorecard identifies something that most current assessment approaches miss: the difference between *measuring inputs* and *measuring system performance*.

This is a fundamentally different analytical lens. It's particularly important for infrastructure, logistics and sustainment, which act as the connective tissue of the northern defence system. A runway without fuel is a car park. A port without a maintenance workforce is a jetty. The scorecard makes such interdependencies visible before they become failures.

How the framework changes decisions

Infrastructure systems

Infrastructure expansion doesn't necessarily improve operational readiness. Additional runway capacity delivers limited advantage if fuel distribution, munitions handling and logistics throughput remain constrained. The framework helps to expose those bottlenecks before investment decisions lock them in.

The scorecard also introduces two measures largely absent from current planning frameworks: time to failure and time to recovery. Those measures show how long systems can operate under pressure and how quickly they can recover once disrupted. In contested environments, those timelines matter as much as the infrastructure itself.

Finally, the framework improves coordination across portfolios. The Defence organisation relies on systems that it doesn't own, including energy, transport, communications and workforce infrastructure. The PRR Scorecard provides a common framework for assessing how those dependencies affect operational resilience.

Logistics systems

Logistics failure rarely begins with physical destruction alone. In contested environments, disruption often starts with degraded coordination, delayed visibility and slowing movement across supply networks. The framework assesses whether logistics systems can continue functioning once those pressures begin to compound. That includes contested maritime access, degraded transport corridors and loss of digital coordination. In northern Australia, that exposure concentrates around Darwin Port, East Arm logistics infrastructure, the Stuart Highway corridor and remote fuel-distribution networks supporting dispersed operating locations.

Scenario testing shows that logistics systems often fail through loss of coordination rather than physical destruction alone. When digital systems degrade, visibility across supply networks narrows and the ability to prioritise, sequence and route movements weakens. The PRR Scorecard makes those dependencies visible before disruption occurs. The framework is particularly relevant in the Northern Territory, where logistics efficiency depends heavily on a small number of transport corridors, contractor networks and fuel-supply pathways operating across vast distances.

Sustainment capability

Sustainment determines whether combat power can endure beyond the opening stages of a crisis. Workforce shortages, fragile supply chains and constrained maintenance throughput often degrade readiness faster than platforms themselves. Those pressures become more acute across remote Northern Territory operating environments where industrial support, repair depth and supply-chain flexibility remain geographically constrained.

The framework focuses on three areas:

- First, it treats workforce availability as a strategic constraint. Sustainment depends on specialised labour, particularly in remote operating environments where workforce depth is limited. In locations such as Darwin and Katherine, workforce depth remains constrained by housing availability, contractor competition, fly-in/fly-out dependence and limited specialist trade pools.
- Second, it assesses whether supply chains remain viable under stress, including dependence on single suppliers, vulnerable transport routes and fragile digital coordination systems.
- Third, it measures how quickly readiness degrades during a prolonged contingency. That allows planners to identify where stockpiling, pre-positioning and sovereign maintenance capacity can improve operational endurance.

The result is a shift in perspective. Sustainment is no longer assessed simply by cost, contracts or peacetime efficiency. It's assessed by whether it continues to function when operational pressure is highest.

Practical applications

Strategy, Policy and Industry Group

For contestability planners in the Defence's Strategy, Policy and Industry Group, the PRR Scorecard tests whether proposed investments translate into operational effect under contested conditions, rather than whether it exists on paper. It helps to answer a fundamental question: what's been built, acquired or funded, and what can the system actually do when subjected to disruption, degradation or sustained pressure?

The framework enables planners to assess whether concepts such as forward basing, rotational presence and dispersed operations remain viable once fuel, logistics, workforce, infrastructure and digital constraints are taken into account. In doing so, it highlights where operational concepts depend on enabling systems that are fragile, overstretched or absent altogether.

The scorecard also helps to identify the infrastructure, industrial, sustainment and workforce investments needed to ensure that force structure decisions deliver the intended operational outcomes and remain sustainable under pressure.

Defence Security and Estate Group

For Defence Security and Estate Group practitioners, the PRR Scorecard strengthens investment cases by linking infrastructure projects directly to operational outcomes. It shifts the argument from asset delivery to operational effect.

Rather than simply demonstrating that a project expands capacity, the framework shows whether it improves resilience, extends endurance or reduces recovery time under disruption. A fuel project, for example, is no longer measured only by storage volume, but by whether it materially improves operational continuity during contested supply conditions.

The framework also exposes projects that fail to resolve the actual constraint within the broader system, allowing investment to be redirected towards the bottlenecks limiting operational performance.

Senior ADF officers

For senior ADF officers, the PRR Scorecard provides a structured way to assess whether a base, group of bases or operating area can sustain operations under pressure. It evaluates infrastructure, energy, logistics, workforce and sustainment as a connected operational system rather than separate functions.

The framework helps commanders identify how long operations can continue before disruption becomes operationally significant, where local mitigation measures are sufficient, and where broader support is required. It also exposes dependencies on external

power, fuel, logistics, workforce and digital systems that sit outside Defence's control but directly affect operational readiness.

Used consistently, the scorecard provides a common preparedness framework for reporting risk, prioritising investment and coordinating with sustainment, logistics and government partners.

Joint Logistics Command

For Joint Logistics Command, the PRR Scorecard identifies where the logistics network is most likely to fail under operational pressure and how quickly it can recover.

The framework assesses ports, fuel hubs, transport corridors and maintenance nodes as part of a connected logistics system rather than as isolated facilities. It highlights the weakest points in the network and identifies where disruption is most likely to cascade across sustainment and force generation.

The time-to-recovery overlay is particularly important. It allows planners to determine whether degraded logistics nodes can be restored within operational timelines or whether additional redundancy, dispersal or surge capacity is required.

The framework also provides a common analytical language for engagement with industry, infrastructure providers and state and territory governments on logistics resilience and sustainment risk.

Regional maintenance centres

For regional maintenance centre practitioners, the PRR Scorecard assesses whether maintenance systems can restore combat capability at the speed and scale that operations require.

The framework focuses on the practical constraints that slow recovery: workforce shortages, industrial throughput limitations, fragile supply chains and reliance on imported components. It identifies whether repair timelines remain within operational tolerance or whether sustainment capacity will degrade faster than it can recover.

The scorecard also highlights where sovereign manufacturing, stockholding, workforce development and supplier diversification would reduce operational risk during prolonged contingencies.

State and territory governments

For State and Territory governments, such as Northern Territory Government practitioners, the PRR Scorecard provides a practical framework for aligning the territory's infrastructure planning with Defence's preparedness requirements.

The framework helps to identify which roads, ports, energy systems, communications networks and workforce investments directly support operational resilience across northern Australia. It also strengthens the case for federal government co-investment by demonstrating where northern infrastructure is load-bearing for defence operations.

Most importantly, the scorecard helps governments sequence investment more effectively by identifying which enabling systems constrain broader operational performance across the north.

Embedding the PRR Scorecard approach

The 2026 NDS assumes that northern Australia can sustain force generation, logistics and recovery under pressure. Current planning systems don't consistently test whether that assumption holds. The PRR approach is intended to close that gap.

The PRR Scorecard framework assesses whether the systems that underpin northern defence can continue generating, sustaining and recovering operational effect under pressure. It focuses on operational performance, not simply infrastructure delivery or capability growth. Its purpose is straightforward: identify where preparedness assumptions fail once systems come under sustained stress.

The framework is intended to sit inside existing planning and investment processes, including the IIP, federal and state government budget cycles, force posture planning, resilience programs and infrastructure investment decisions.

Its role is to provide a common preparedness framework across portfolios and agencies so that infrastructure, sustainment, workforce and capability investments reinforce one another rather than develop in isolation.

Recommendation for a pilot program

The methodology should be tested against a limited number of high-consequence operational problems before its wider adoption. The objective is simple: determine whether the framework improves real investment and preparedness decisions.

Step 1: Scope the pilot

Select two or three domains where existing data is most accessible and where the decision-making stakes are clearest. The strongest candidates for a pilot are:

- *Fuel and energy security (Tier 1)*, because the interdependencies are well documented, the failure pathways are legible, and policy decisions in this domain are live and consequential.
- *Logistics and sustainment (Tier 1)*, because it sits at the intersection of Defence and civilian systems and is directly exposed to compounded disruption scenarios.

- *Workforce and human capital (Tier 3)*, because it's identified as the most persistent and least substitutable constraint, and because existing data from the Defence Industry Security Program, the IIP and Northern Territory infrastructure programs is available to inform assessment.

Step 2: Assemble a small, cross-agency analytical panel

Draw up to six practitioners from the profiles identified in the preceding section. That's sufficient to test whether the methodology produces consistent and credible outputs without creating the coordination burden that would slow a first iteration. The panel should include at least one Defence planner, one estate or logistics practitioner, and one state or territory counterpart to ensure that the cross-institutional dependencies that the PRR Scorecard maps are represented in the assessment itself.

The panel should also include at least one Northern Territory Government representative as a full participant rather than as a consulted stakeholder, recognising that many of the systems underpinning northern defence preparedness, including transport corridors, ports, workforce development, housing and energy infrastructure, sit outside the Defence organisation's control. Western Australia and Queensland should be engaged early in the pilot process to support future expansion beyond the Northern Territory.

Step 3: Apply the scoring methodology to one scenario first

Rather than producing a full domain-by-domain assessment, apply the PRR matrix across two or three pilot domains against a single, well-defined operational scenario. That tests whether the scoring produces useful differentiation, whether the narrative evidence requirement is manageable, and whether the time-to-failure and time-to-recovery overlays can actually be populated with available data. A scenario involving supply disruption to a northern operating base under sustained operational pressure is a practical starting point: it's demanding enough to stress the enabling system without requiring access to the most sensitive operational planning assumptions.

Step 4: Test the output against a real decision

The critical validation step is whether the PRR Scorecard output changes or sharpens an actual investment or sequencing decision. Strong candidates include a current IIP sequencing question, a Northern Australia Infrastructure Facility funding assessment, or a co-investment decision under the US Force Posture Initiative. The test isn't whether the scores are correct; it's whether they give decision-makers better visibility of trade-offs than they currently have.

Step 5: Document what the methodology can and can't assess

Every first-instance application will surface data gaps, classification barriers and contested judgements. Those are features, not failures. Documenting them explicitly is how the pilot produces value beyond its immediate outputs: it maps where data-sharing arrangements need to be formalised, where classification levels prevent cross-agency analysis, and where the scoring descriptors require refinement before the methodology can be applied with confidence across the broader domain set.

Step 6: Identify where the ownership of the PRR Scorecard logically sits

The pilot will generate durable value only if responsibility for maintaining and applying the PRR Scorecard is clearly assigned before the pilot concludes. Ownership shouldn't default to the agency that convened the pilot; it should be assigned to the body best positioned to sustain the analytical function, secure the data-sharing relationships that the methodology requires, and ensure that outputs reach the decision-making forums where they matter.

The strongest candidate for initial custodianship is Defence's Resilience Division, which has the cross-portfolio mandate, access to data and relationship architecture needed to anchor the methodology within the IIP and force posture cycles.

However, the pilot is also likely to demonstrate that many of the dependencies identified by the PRR Scorecard extend beyond Defence's direct responsibilities. Fuel supply, energy security, transport infrastructure, workforce availability, industrial capacity and critical digital systems are influenced by decisions taken across multiple federal portfolios, state and territory governments, industry and infrastructure operators.

Over time, the PRR Scorecard should evolve beyond a Defence-owned analytical tool towards a broader cross-government preparedness framework. A longer term governance model could include Defence, Prime Minister and Cabinet's National Security Division, Home Affairs, Foreign Affairs and Trade, Treasury and relevant state and territory governments, reflecting the distributed ownership of the systems that underpin national resilience. Without such arrangements, the PRR Scorecard risks identifying vulnerabilities that no single agency has the authority or responsibility to address.

To ensure that findings inform decision-making across jurisdictions, consideration should also be given to tabling PRR assessments through existing national-security coordination mechanisms, including the state and territory committees. This would provide a standing forum through which preparedness risks, interdependencies and investment priorities can be considered collectively by the governments responsible for managing them.

The institutional challenge

The PRR Scorecard is designed as an assessment framework, but its findings expose a broader institutional challenge. The vulnerabilities most likely to constrain northern defence preparedness don't sit neatly within Defence's direct control. As pointed out above, fuel security, energy resilience, transport infrastructure, workforce availability, housing, industrial capacity, digital networks and critical supply chains are shaped by decisions taken across multiple Commonwealth portfolios, state and territory governments, industry and infrastructure operators.

That creates a structural problem. Defence can identify dependencies and assess risk, but it doesn't own many of the systems on which operational effectiveness depends. A PRR Scorecard may successfully identify vulnerabilities, prioritise investments and reveal critical points of failure, yet still fail to improve preparedness if there's no governance mechanism capable of acting on the findings across institutional boundaries.

That challenge isn't unique to Australia. Finland's National Emergency Supply Agency, Sweden's Civil Contingencies Agency and other 'total defence' models recognise that resilience can't be managed solely within defence organisations. They provide enduring mechanisms that connect government, industry and infrastructure operators around a shared understanding of national preparedness.

The PRR Scorecard should therefore be viewed as more than a Defence planning tool. While Defence is the logical starting point for piloting and refining the methodology, the dependencies that it assesses extend across the broader national defence enterprise. Over time, the framework should evolve into a cross-government preparedness mechanism capable of informing investment, policy and risk-management decisions across the systems that underpin Australia's northern operating environment.

The ultimate value of the PRR Scorecard won't be measured by the quality of the assessments it produces, but by whether those assessments are connected to institutions capable of coordinating action across the full preparedness ecosystem. The scorecard can reveal where the system is fragile. The longer term challenge for government is ensuring that there's a governance architecture capable of responding to what it reveals.

Rollout framework

Following pilot completion and methodology refinement, institutionalisation should proceed in two phases. Expansion should occur only once analytical outputs are stable and data-sharing arrangements function reliably.

Phase 1: Establishment and validation

The initial phase is deliberately narrow in scope and operationally focused. Its purpose isn't to produce a definitive preparedness picture immediately, but to validate whether the PRR Scorecard framework improves the visibility of systemic vulnerabilities, investment trade-offs and preparedness gaps in practice, and to build the analytical trust that broader participation over time will require.

Governance in this phase should be anchored in the relevant federal government defence and resilience functions, and day-to-day analytical support should be drawn from force posture, estate planning, logistics and operations planning. The inclusion of a locally embedded operational perspective from the outset is essential: leaving out ground-level situational awareness of the enabling environment, such as infrastructure constraints, workforce availability and logistics conditions, would risk scoring domains against planning assumptions that don't reflect conditions on the ground.

The effectiveness of this phase turns on three conditions. The methodology must be analytically credible and produce outputs that practitioners recognise as accurate. Meaningful data access must be secured across relevant classified systems and civilian planning inputs. And outputs must consistently reach the decision-making forums where investment and prioritisation decisions are actually made. Without all three, the PRR Scorecard risks becoming a reporting exercise rather than an operational preparedness tool.

During this phase, the framework is tested against a defined set of capability, infrastructure and sustainment challenges. It's also during this phase that information-sharing arrangements with SOCI-regulated providers, covering energy, water, transport, communications and key infrastructure, should be established. SOCI-regulated operators hold the operational data on civilian system performance that the framework's external dependence overlays require but that government agencies can't generate alone. Engaging them as analytical contributors rather than passive subjects of assessment, structured through existing SOCI reporting mechanisms, allows the framework to incorporate ground-truth information on redundancy levels, failure modes and recovery timelines without creating parallel obligations.

Towards the latter part of this phase, engagement with the broader private-sector enabling base, such as industry primes, logistics and fuel contractors, construction and engineering firms and workforce providers, should be scoped and, where appropriate, initiated.

The Defence Industry Security Program provides a relevant existing framework for managing that engagement without compromising commercial confidentiality. The objective is to establish structured information-sharing arrangements that allow commercial operational data to inform domain scoring in Phase 2.

Phase 2: Geographical expansion

Once the methodology is validated, data-sharing arrangements are operational and analytical outputs have demonstrated credibility with relevant decision-making forums, the framework expands geographically to encompass the full northern Australia operating environment.

Expansion proceeds first to incorporate the Western Australian dimension of that environment. Western Australia's strategic depth—its naval, air, logistics and industrial infrastructure across the Pilbara, Kimberley and southern base network—is loadbearing for force generation and sustainment across northern Australia. The logistics and sustainment and industrial base domains require a Western Australian dimension to accurately reflect the distribution network and maintenance capacity available to joint forces operating across the north.

Expansion to Queensland completes northern Australia coverage, incorporating the training, port, industrial and logistics infrastructure, including the significant ADF–partner nation exercise and operations footprint in the state's north, that sits beyond the Northern Territory framing of Phase 1. The workforce and human capital domain benefits particularly from that extension, given the scale of defence-related employment and training infrastructure in Queensland's north.

Expansion in both cases should be coordinated with relevant state-level infrastructure, resilience and industry planning frameworks to ensure that PRR Scorecard outputs engage, and don't duplicate, existing state preparedness work.

The cumulative aim of both phases is the development of a more integrated preparedness architecture: one capable of linking national-security planning, economic resilience, infrastructure investment and continuity preparedness within a shared analytical framework. That architecture should reflect the whole-of-nation character that the strategic environment demands and give governments, agencies and industry the common foundation needed to act on it.

Implications for national defence

The PRR Scorecard provides a practical method for assessing preparedness, resilience and redundancy across the northern defence system. However, the report's central finding is ultimately institutional rather than analytical. Northern defence preparedness depends on systems that extend well beyond the Defence organisation itself. The challenge is therefore not only to identify vulnerabilities, but to build the governance arrangements capable of addressing them. The credibility of Australia's strategy of denial will depend not simply on what Defence can do alone, but on whether government, industry and society can function together as an integrated preparedness system.

Conclusion

Over the past decade, Australia has invested heavily in northern infrastructure, alliance integration and force posture expansion. Those investments have increased capacity. However, they haven't always increased operational resilience at the same pace. Current assessment approaches still measure infrastructure delivery more effectively than they measure whether the broader northern operating environment can sustain prolonged disruption, absorb cascading failure or recover operational tempo once systems begin degrading simultaneously.

The PRR Scorecard responds to that gap. Its purpose isn't to create another reporting mechanism or resilience framework. Its purpose is to identify which constraints limit operational viability and which investments materially improve force sustainment, recovery and continuity during disruption.

This report demonstrates that vulnerability rarely emerges through a single catastrophic event. It develops through interactions among fuel, logistics, infrastructure, workforce and digital systems operating with limited redundancy across vast distances. In northern Australia, geography magnifies those pressures. Distance increases fuel demand, slows recovery, narrows logistics flexibility and reduces surge capacity once disruption begins.

Australia's northern defence posture also depends increasingly on civilian infrastructure, commercial logistics networks and workforce systems never designed for sustained strategic disruption. Fuel distribution, freight movement, contractor availability, transport corridors and energy reliability now shape defence preparedness as directly as do bases, ports and runways. They're no longer supporting functions. They're national security.

The challenge now is practical implementation. Governments need a disciplined way to identify where operational assumptions might fail, where redundancy is absent and where investment sequencing matters most before disruption exposes those weaknesses in real time.

Northern Australia already carries enormous strategic weight within Australia's defence posture. The remaining question is whether the systems that underpin that posture can sustain prolonged operational demand once disruption begins.

The risk for Australia isn't that northern Australia lacks strategic value. The risk is assuming that strategic value automatically translates into operational resilience.

Glossary

A **domain** is a functional system that contributes to defence capability. It's tangible and accessible, it has inputs, outputs and performance characteristics and it can be scored across preparedness, resilience and redundancy.

Infrastructure assets are the physical and fixed built environment needed to support operations and service delivery. That includes, but isn't limited to, runways, roads, ports, housing, power grids, water systems and communications infrastructure. Infrastructure assets are typically capital-intensive, long-lived and place-based, and their availability, condition and capacity directly affect operational and strategic outcomes.

Logistic systems are the networks, processes and capabilities that plan and execute the movement and supply of personnel, equipment and materiel. Logistics systems are fundamentally concerned with flow—getting the right people, equipment and supplies to the right place at the right time. They include fuel networks, transport corridors, distribution networks and alliance logistics arrangements.

National Defence is a coordinated whole-of-government and whole-of-nation approach to meet the strategic challenges that Australia faces, including the threat of conflict and the prospect of coercion.[30]

The **northern Defence operating environment**, for the purposes of this report, is defined by the *Northern Australia Infrastructure Facility Act 2016* (Cth) as all the Northern Territory and those parts of Queensland and Western Australia that intersect with the Tropic of Capricorn, Christmas Island and the Cocos (Keeling) Islands, collectively referred to as the 'Indian Ocean territories'.[31]

Planners operate at the level of execution, translating intent into sequenced, resourced and deliverable actions. They work within defined parameters to coordinate activities, manage dependencies and deliver outcomes efficiently and on time. Their focus is on feasibility and implementation, ensuring that what's been decided can actually be done, at scale and under real-world constraints.

Policymakers shape the system within which action occurs, defining the rules, incentives and trade-offs that guide behaviour across government, industry and society. They operate in conditions of ambiguity, balancing competing priorities while translating political intent into frameworks that are practical, legitimate and enforceable. Their work determines how actors behave and what outcomes are enabled—or constrained—over time.

Preparedness is about anticipation and readiness. It's the deliberate work undertaken in advance to ensure that the Defence organisation can respond quickly and effectively when something happens.

Redundancy is one of the mechanisms used to achieve resilience by deliberately building extra capacity or alternative options into systems so that if one component fails, another can take over.

Resilience is about absorbing shock and continuing to operate when systems are under stress.

Strategists define direction under uncertainty, identifying what matters most and how advantage or resilience can be secured over the long term. They operate across interconnected systems, assessing how economic, security and institutional dynamics interact, and determining where to prioritise effort and accept risk. Their role isn't to optimise within the system, but to shape it—ensuring that policy and planning align with a coherent strategic purpose.

The **Strategy of Denial**, as defined by the 2026 NDS, aims to deter any conflict before it begins, prevent any potential adversary from succeeding in coercing Australia through force, support regional security and prosperity and uphold a favourable regional strategic balance. It guides Defence's contribution to National Defence and spans all five domains: maritime, land, air, space and cyber.

Sustainment capabilities are the human, technical and organisational enablers that maintain forces in an effective and operationally ready state over time. Sustainment capabilities are fundamentally concerned with endurance, keeping forces supported, viable and capable for as long as operations require. That includes skilled labour, energy supply, power generation, data links, and maritime and air sustainment capacity.

A **tier** is a prioritisation layer that reflects how critical a domain is to operational success. It isn't a separate system, but a way of ranking domains based on their role in operational viability, sustainment and scale. Tiers reflect sequences of failure under stress, they highlight what matters first, most and longest and they guide investment and policy prioritisation.

Users are the individuals or organisations engaging with the PRR Scorecard in an assessment, planning, advisory or decision-making capacity (they can include policymakers, planners and strategists). The term is intentionally broad and encompasses actors across the federal, state and territory governments and other bodies with relevant policy, operational or strategic responsibilities. No specific organisational affiliation or seniority level is assumed.

Notes

1 Defence Department, *2026 National Defence Strategy*, Australian Government, 2026, 41, online.
2 JH Holland, 'Complex adaptive systems', *Daedalus*, 1992, 121(1):17–30, online.
3 E Ostrom, 'A diagnostic approach for going beyond panaceas', *Proceedings of the National Academy of Sciences*, 2007, 104(39):15181–15187, online.
4 C Perrow, *Normal accidents: living with high-risk technologies*, Basic Books, 1984.
5 M Ouyang, 'Review on modeling and simulation of interdependent critical infrastructure systems', *Reliability Engineering & System Safety*, 2014, 121:43–60, online.
6 AW Gray Jnr, 'Joint logistics in the Pacific theater', in A Gropman (ed.), The big 'L': *American logistics in World War II*, National Defense University Press, 1997, 293–337.
7 Christopher M Rein, *Multi-domain battle in the Southwest Pacific theatre of World War II*, Combat Studies Institute Press, 2017.
8 SV Buldyrev, R Parshani, G Paul, HE Stanley, S Havlin, 'Catastrophic cascade of failures in interdependent networks', Nature, 2010, 464:1025–1028, online.
9 Perrow, *Normal accidents: living with high-risk technologies*.
10 Defense Department, *Joint Concept for Integrated Campaigning*, US Government, 2018, online.
11 SM Rinaldi, JP Peerenboom, TK Kelly (2001). 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, 2001, 21(6):11–25, online.
12 I-Cheng Lin, Osman Yagan, Carlee Joe-Wong, 'Dynamic coupling strategy for interdependent network systems against cascading failures', *arXiv*, 2022, online.
13 R Guidotti, P Gardoni, Y Chen, 'Modelling the resilience of critical infrastructure: the role of network dependencies', *Sustainable and Resilient Infrastructure*, 2016, 1(3–4):153–168; D Duan, HE Stanley, J Gao, SV Buldyrev, 'Universal behaviour of cascading failures in interdependent networks', *Proceedings of the National Academy of Sciences*, 2019, 116(45):22452–22457.
14 RR Liu, M Li, CX Jia, BH Wang, 'The "weak" interdependence of infrastructure systems produces mixed percolation transitions in multilayer networks', *Scientific Reports*, 2018, 8, article 10834.
15 Department of Homeland Security, *National Infrastructure Protection Plan 2013: partnering for critical infrastructure security and resilience*, US Government 2013, online.
16 Organisation for Economic Co-operation and Development (OECD), *Good governance for critical infrastructure resilience*, OECD Publishing, Paris, 2019, online.
17 Cabinet Office, *National Risk Register 2025*, UK Government, 2025, online.
18 'Deterrence and defence: resilience and civil preparedness', NATO, 2025, online.
19 Ministry of National Defence, *National Security Strategy of the Republic of Lithuania*, Lithuanian Government, 2021.
20 State Comptroller of Israel, 'The state's preparedness for an earthquake: national infrastructure resilience', Israeli Government, 2024.
21 Federal Emergency Management Agency, *National Preparedness System*. US Government, 2020, online.
22 'Resilience and civil preparedness', NATO, 2024, online.
23 Cabinet Office, *National Risk Register 2025*.
24 National Infrastructure Commission, *Anticipate, react, recover: resilient infrastructure systems*. UK Government, 2020.
25 National Emergency Supply Agency, 'Main tasks of the National Emergency Supply Agency', Finnish Government, 2026, online.
26 Swedish Civil Defence and Resilience Agency, 'The strategic environment and planning assumptions for Swedish Total Defence 2025–2030', Swedish Armed Forces, 2026, online.
27 Ministry of Defence, 'Total Defence: our first line of defence', Singaporean Government, 2025, online.
28 Cabinet Secretariat, *National Resilience Basic Plan*, Japanese Government, 2019.
29 Department of Home Affairs, '*Security of Critical Infrastructure Act 2018*: risk management program guidance, Australian Government, 2023, online.
30 Defence Department, 2026 *National Defence Strategy*.
31 *Northern Australia Infrastructure Facility Act 2016* (Cth), online.

Acronyms and abbreviations

ADF	Australian Defence Force
DSR	Defence Strategic Review
FEMA	Federal Emergency Management Agency (US)
IIP	Integrated Investment Program
NATO	North Atlantic Treaty Organization
NDS	National Defence Strategy
OECD	Organisation for Economic Co-operation and Development
PRR	preparedness, resilience and redundancy
SOCI Act	*Security of Critical Infrastructure Act 2018* (Cth)


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
25
YEARS
2001–2026