Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Annual Risk Review

Third Edition
November 2025

Contact us

Enquiries regarding the licence and any use of this document are welcome to enquiries@CISC.gov.au, or:

Risk Assessment Branch
Critical Infrastructure Security Centre
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

Foreword

The Australian Government's Critical Infrastructure Annual Risk Review for 2025 covers the breadth of threats and hazards faced by Australia's critical infrastructure over the past 12 months. It provides guidance on emerging and enduring risks that impact our national security and economic prosperity. The review is designed for a diverse audience across all levels of industry, government, and the broader community.

Through the insights and information in this review, critical infrastructure owners and operators will be better equipped to understand the risks from cyber, human and physical threats, and from supply chain hazards and natural disasters. Maintaining a clear awareness of these risks is vital to protect the essential services we all rely on.

Critical infrastructure networks globally are increasingly targeted by malicious actors and Australia is not immune. Geopolitical tensions are placing pressure on democracies and the reliable delivery of essential services and supply chains. Cyber incidents remain one of the fastest growing threats to our nation, and inadvertent human error or system failures are often proving as disruptive as deliberate malicious activity. Our future critical infrastructure is being shaped and strengthened through technological advancements, with Australia actively investing in artificial intelligence implementation and the development of quantum computing. However, Australia's critical infrastructure must remain vigilant against the new threats and risks these technologies will bring.

The Australian Government is committed to safeguarding the nation against threats and hazards that could disrupt our critical systems. To strengthen cyber resilience, we have implemented the Cyber Security Act 2024 and launched the Commonwealth Cyber Security Uplift Plan to elevate government agency cyber security through updated standards. More than 200 critical infrastructure assets have been declared Systems of National Significance with enhanced cyber security obligations. These measures reinforce the Government's commitment to securing Australia's cyber environment and protecting critical infrastructure.

This is not something Government can do alone. We work side by side with industry to continually strengthen our critical systems, to safeguard national security and economic prosperity. Industry is actively enhancing the security of critical infrastructure through targeted investment, addressing vulnerabilities, strengthening systems and securing sensitive data – efforts that are both essential and commendable.

Looking ahead, strong partnerships between industry and government will ensure Australia remains resilient to emerging risks and well-positioned to protect the safety and prosperity of future generations.

The Hon. Tony Burke MP
Minister for Home Affairs, Minister for Immigration and Citizenship,
Minister for Cyber Security

About the Critical Infrastructure Security Centre

Within the Department of Home Affairs, the Critical Infrastructure Security Centre (CISC) drives an all-hazards approach to collaboratively ensure the security, continuity and resilience of Australia's critical infrastructure. We actively assist Australian critical infrastructure owners and operators to understand the risk environment, meet their regulatory requirements and maintain secure and resilient services for the shared benefit of all Australians.

Eye on the horizon – delivering national security for today

The CISC holds a unique and detailed understanding of the national security risks faced by critical infrastructure. We draw on our partnerships across government, industry and the community to monitor issues and identify trends to understand the current risk environment. Our expertise includes forecasting changes in the risk landscape through scenario analysis and assessing the potential impacts on critical infrastructure. We leverage this knowledge to provide timely assessment to inform and guide our stakeholders.

Establish trusted partnerships

The best outcomes for Australia are achieved when government and industry work together towards a collective goal. Through the CISC's Trusted Information Sharing Networks, we support critical infrastructure asset owners and operators to prepare for and respond to hazards that may prejudice Australia's national interests or assured delivery of essential goods and services.

We connect critical infrastructure owners and operators to ensure an understanding of dependencies and to reinforce resilience through collaboration. Our partnerships extend across federal, state and territory government agencies, including through the facilitation of shared exercises, providing expert briefings and developing tools to prepare for and recover from a crisis. Regular information sharing between critical infrastructure operators and government is evidence of a strong and trusted partnership model.

Promote best-practice regulation

Effective regulation for critical infrastructure security requires a cooperative approach, working with industry and government to deliver regulatory functions that jointly manage risks. We support standards, accreditation, and regulatory reform, and work with other regulators operating within critical infrastructure sectors to ensure we fully consider the security and risk management of each asset.

We harness our regulatory and policy expertise and influence to work with industry to minimise harm. Our regulatory approach is adaptable and seeks to set appropriate standards for managing risk; we ensure compliance through a combination of education, information sharing and ongoing monitoring to verify regulatory settings are correct.

Our regulatory responsibilities are drawn from: *Security of Critical Infrastructure Act 2018 (SOCI Act)*; *Aviation Transport Security Act 2004*; *Maritime Transport and Offshore Facilities Security Act 2003*; *AusCheck Act 2007*; and *Cyber Security Act 2024*.

Provide tailored guidance for critical infrastructure

Our specialised expertise, strong partnerships and regulation allow us to provide unique and world-leading guidance to critical infrastructure owners and operators. Some of this work includes:

- The Critical Infrastructure Resilience Strategy is a framework for how we work together to mature the security and resilience of critical infrastructure.
- AusCheck provides fast, fair and reliable background-checking services.
- The 2023-2030 Australian Cyber Security Strategy outlines the government's strategy for building Australia's cyber resilience.
- The Foreign Ownership, Control, or Influence Risk Assessment Guidance helps to manage potential risk posed by vendors operating in supply chains.

More information, guidance and tools can be found on the CISC website.

Introduction

The third edition of the CISC's Critical Infrastructure Annual Risk Review outlines key risk-driven issues that have impacted the security of Australia's critical infrastructure in 2025.

Risk issues are presented for the hazard categories: cyber and information security; supply chain hazards; physical security; natural hazards; and personnel security, as per the detail provided in the SOCI Act and accompanying rules for Critical Infrastructure Risk Management Programs (CIRMP) and further defined below.

An uncertain risk landscape

Geopolitical risk is an ongoing reality for all critical infrastructure sectors. Instability and insecurity of operational environments are deepening existing fractures and creating new ones domestically and internationally, changing the way we approach risk. In addition, socio-political and demographic divides, along with rapidly changing digital and technological environments, are eroding trust in democratic institutions.

In 2025, the risk landscape is defined by escalation of the risks that were identified in the 2024 Critical Infrastructure Annual Risk Review. Government and industry alike have had to anticipate and be ready to respond to disruption from a wide range of hazards, including from unpredictable changes in the global geopolitical environment and the emerging security implications of novel technology.

Record numbers of reported **cyber** incidents have established this threat as part of standard business processes. Australia's digital infrastructure is on the frontline for critical infrastructure security.

Critical infrastructure is adapting to a multipolar global environment that is placing additional pressure on **supply chains** that are already characterised as long, concentrated, complex and opaque.

The **physical** sabotage of critical infrastructure is at the forefront in many global conflicts, with readily accessible technologies and grey zone tactics proving effective alongside traditional military capability.

Climate change continues to create uncertainty for risk management. Severe weather is impacting in more unexpected locations, and repeated consequences from different **natural hazards** are squeezing Australia's response and recovery capabilities.

Accidents, technical errors and challenges in meeting skilled workforce requirements are creating more disruptive **personnel** security effects alongside threats from malicious insiders.

Geostrategic shifts are a hurdle for risk management decision-making

Australia is inextricably linked economically to the rest of the world, with these connections forming a critical foundation of our economy. While an ambiguous and complex geostrategic environment is not new, the current uncertainty around geopolitical actions and market response mechanisms impedes our ability for short-term planning.

We are reliant on global trade for digital technology and devices, critical components, chemicals, liquid fuels and medical supplies. We are supported by offshore service providers, infrastructure (such as submarine cables), contractors and expertise that keep us connected across the globe. However, this also means that global conflict, tensions and instability create risks that challenge our physical and digital resilience.

In 2025, international supply chains for software and hardware have left us vulnerable to harmful activity, both deliberate and inadvertent. Australia's role in debating global issues has also exposed us to potential retribution from perceived adversaries, ranging from plausibly deniable grey-zone tactics to preparation for an act of state-sponsored sabotage.

Overseas conflict has impacted domestic community sentiment and eroded social cohesion, increasing the likelihood of politically motivated violence, the threat of lone-actor extremism, ideologically motivated vandalism and small-scale sabotage has persisted.

Resilience in the face of rapid technology change

Geopolitics is accelerating global technology transformation. In many areas of next-generation technologies, we are experiencing geostrategic competition for technology leadership and influence. Critical infrastructure needs to address multiple, fast-moving geopolitical, technological and societal events. Anticipating risks and building resilience in the face of this change is a high priority.

Technology advancements offer both risk and reward. The sheer volume of commentary on technology changes and development of operational technology is leaving critical infrastructure security decision makers with tough, and at times conflicting, choices about where to focus resilience efforts.

Artificial intelligence (AI) is already driving national policy agendas, infrastructure innovation and societal concern. Realising the opportunities of AI will require mitigating the new threats it introduces, while balancing existing information technology (IT) security measures.

Greener technologies are a priority for government policy increasing Australia's dependency on renewable electricity generation. This requires technological transformation in much of our existing infrastructure, and competition for resources and technology that underpins it.

Navigating the best course of action

Where does this leave critical infrastructure security and risk planners going forward? It is vital that our approach to security management acknowledges and anticipates these risks, and that business continuity plans are robust and resilient to mitigate the impacts for when, not if, they occur.

Critical infrastructure owners need to adapt risk management strategies to meet shifting dependencies, short-term and long-term supply chain disruptions and geopolitical tensions. Risk mitigation now requires an acceptance and incorporation of technology competition, supply concentration and unavoidable third-party risk.

The 2025 Critical Infrastructure Annual Risk Review underpins a strategic understanding of the risks to Australia's critical infrastructure and their impact on operational delivery.

CIRMP Hazard Definitions

Cyber and Information security hazards include where a person, whether authorised or not: (a) improperly accesses or misuses information or computer systems about or related to the critical infrastructure asset; or (b) uses a computer system to obtain unauthorised control of, or access to, the critical infrastructure asset that might impair its proper functioning.

Supply Chain hazards include malicious actions to exploit, misuse, access or disrupt the supply chain; an over-reliance on particular suppliers, and other disruption from issues in the supply chain, including a failure or lowered capacity of supply.

Physical security hazards include the unauthorised access to, interference with, or control of critical infrastructure assets, to compromise the proper function of the asset or cause significant damage to the asset.

Natural Hazards include damage or disruption from fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic).

Personnel security hazards include where a critical worker acts, through malice or negligence: (a) to compromise the proper function of the asset; or (b) to cause significant damage to the asset.

Risk and Regulation

Risks that impact the social or economic stability of Australia or its people, or that have the potential to undermine Australia's national security and resilience need to be considered in critical infrastructure providers' existing risk management strategies. The requirement to establish and maintain a CIRMP not only supports compliance requirements but leads to better security and resilience outcomes for Australia and contributes to a more effective approach for managing your risk.

Uplift your risk management plan

The CISC remains committed to support and guide industry in ways to continually improve CIRMPs. Regulated critical infrastructure owners need to review risk management plans annually and demonstrate a solid understanding of the threats, hazards and vulnerabilities facing operations and how appropriate controls have been put in place to mitigate risk.

Some areas to consider when completing your CIRMP include:

- Identifying significant risk issues with a level of detail will provide a greater level of context to the relevant impacts to critical assets and better guide ongoing mitigation strategies.
- Ensure risk frameworks maintain commensurate levels of maturity across all-hazards, using risk-specific metrics and standards where possible.
- Look for risk management strategies that focus on achieving a high level of availability of critical services.

Ensuring a well-developed risk management plan will extend a higher degree of risk and resilience maturity across all areas of your business and also help to mitigate any incident potentially cascading across your operations or to other sectors.

For additional information, read the CIRMP guidance on the CISC website.

Enhanced reputation

Providing detailed information in your CIRMP goes beyond just meeting regulatory compliance obligations. A risk management plan that has been carefully considered and adapted to the requirements of your operations demonstrates your commitment to high levels of security and resilience of critical operations.

Risks that affect Australia's national security and resilience are as important as business risk in effective critical infrastructure risk management strategies. By integrating an all-hazards approach to risk, you elevate your reputation as a leading provider of secure and trusted national critical infrastructure, building a stronger reputation.

Commercial advantage

Critical infrastructure providers already manage a wide range of risks to their operations. A focus on national security risk may differ from the way risk has been viewed in the past (for example, with financial and commercial interests as a focal point). However, proactively framing risk in a national security context (within existing risk management strategies) will help efforts to improve Australia's national security and socioeconomic resilience and will allow you to stay ahead of the curve of rapidly advancing technologies and the risk this brings. A risk management approach focussed on availability of critical services, now and in the future, helps build trust among the community and government in how these critical services are delivered.

Access to valuable insights

The more detail you can provide as part of risk management plan reporting helps us identify risk management trends and inform the development of practical guidance back to you. More than this, it helps us make well-informed decisions and gives you access to more valuable security insights. Achieving better security outcomes for Australia is a shared goal and ensuring a high level of information sharing is a key contributor to this objective.

Risk Prioritisation

Risk prioritisation enables improved resource allocation, enhanced decision-making, and a more proactive and efficient risk management approach. With resources often limited, risk prioritisation helps organisations break risk into manageable parts that can be built into an effective risk management strategy.

Prioritising how risks are managed is ideally based on an organisation's chosen risk tolerance. This should not be a one and-done process; it needs to adapt with the strategic risk environment and the organisation's changing objectives. Depending on shifting internal and external factors, you may wish to incorporate one of the risk prioritisation strategies outlined below into your enterprise risk management processes:

- **Impact-led approach**: considering risks causing the most damage or disruption to the delivery critical operations.
- **Likelihood-led approach**: considering risks that are more likely to occur, or occur more frequently, but may have varied levels of impact.
- **Cost-led approach**: considering risks with a higher level of monetary impact to an organisation.
- **Resource-led approach**: considering risks that can be addressed with readily available resources (personnel, equipment and funding).

This report includes visualisations comparing risks common to all sectors for each of the five hazards: Cyber/Information, Supply Chain, Physical, Natural Hazard, and Personnel. These visualisations may assist critical infrastructure owners and operators to prioritise risk management across all hazards.

The graphics (Figures 2 to 6) compare the risk issues identified in this report by plotting qualitative assessments of plausibility and damage for each risk. This draws on the CISC's understanding of the national critical infrastructure risk landscape and reflects an all-hazard approach.

- **Plausibility.** Reflects risk likelihood, based on CISC's analysis of a threat or hazard impacting critical infrastructure sectors. Plausibility considers the threat or hazard and the vulnerability of critical infrastructure to that threat or hazard.
- **Damage.** Reflects CISC's analysis of the broad consequence for critical infrastructure sectors, based on worst-case impacts that could arise from the threat or hazard.

Top 5 risk issues by PLAUSIBILITY

1. Third-party cyber risk | *Cyber/Information*
2. Unexpected severe weather location and frequency | *Natural Hazard*
3. Significant disruption from interdependent infrastructure | *Natural Hazard*
4. Extreme-impact cyber incident | *Cyber/Information*
5. Geopolitically driven supply chain disruption | *Supply Chain*

Top 5 risk issues by DAMAGE

1. Extreme-impact cyber incident | *Cyber/Information*
2. Risk from IT/OT/IoT connectivity | *Cyber/Information*
3. Disrupted fuel supply | *Supply Chain*
4. State-sponsored sabotage | *Physical*
5. Significant disruption from interdependent infrastructure | *Natural Hazard*

Sector Interdependency

Critical infrastructure sectors are increasingly interdependent, which is making analysis and treatment of risk more nuanced. Each year, the Critical Infrastructure Annual Risk Review focuses on a particular interdependency issue that has been front-of-mind over the previous 12 months (Figure 1).

Over 2025, global supply chain dependencies subject to third-party and geopolitical disruption are a key risk concern for all critical infrastructure sectors. Dependencies affect all activities and layers of an organisation: operations, corporate and the digital systems that support and link them. Global and third-party dependencies also include risk factors that are less transparent and sit beyond spheres of control.

The geography of liquid fuel dependency

Australia depends on international production and refining for most of our liquid fuels and this supply chain is frequently exposed to geopolitical instability. Diesel is often critical for maintaining assets, fleets and supply chains and, for primary and backup electricity supply. In 2024, Australia's top 5 diesel import countries were South Korea, Malaysia, Singapore, Taiwan and India. Most of the crude oil refined in these countries was sourced from the Middle East, with smaller amounts from the United States, with India and China sourcing significant proportions of crude oil from Russia. Around 13% of diesel was refined in Australia's two remaining refineries.

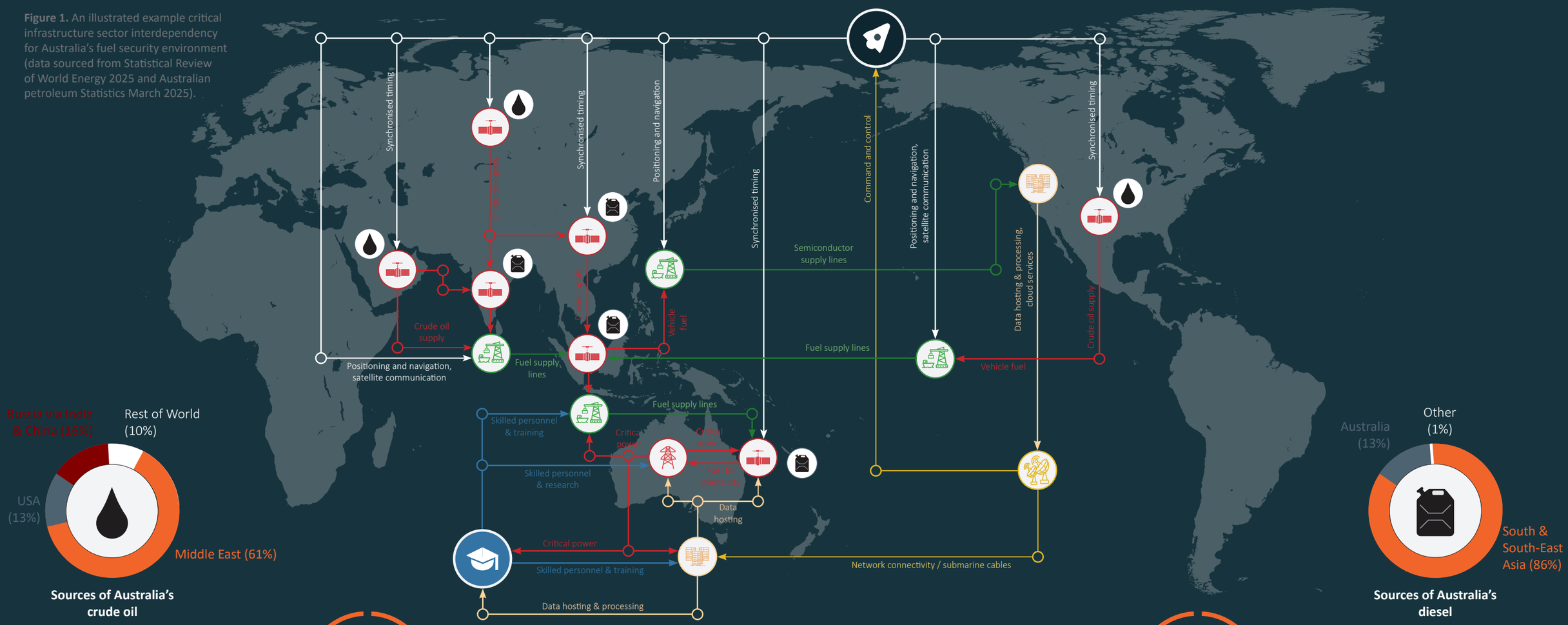
People matter

Critical infrastructure organisations depend on a supply chain for recruiting and maintaining suitably qualified and trained personnel. Across all critical infrastructure sectors, sourcing a steady supply of suitably qualified people face similar global pressures to that of other elements of critical supply. This interdependency includes access to specialised and qualified people, and the provision of skills and capabilities provided by other sectors and third-parties. This network of dependencies not only faces global pressures, but is also managing technology change for workforces, such as the application of AI in parts of operations.

The digital environment

Telecommunications, space-based capabilities and, data and cloud service providers are third-party dependencies across critical infrastructure sectors. Disruption to these dependencies can easily cascade to wider disruption or undue influence. A few large service providers dominate the global market in these sectors and face their own global pressures. In recent years have seen service providers make technical errors, unannounced decisions on service delivery, or face cyberattacks with global impacts. Technical system outages in one organisation can and have had cascading impacts on interconnected critical infrastructure leading to significant global disruptions.

Figure 1. An illustrated example critical infrastructure sector interdependency for Australia's fuel security environment (data sourced from Statistical Review of World Energy 2025 and Australian petroleum Statistics March 2025).




CYBER / INFORMATION

Cyber / Information

CI1 High volumes of cyber incidents are diverting focus from preparation for incidents with extreme operational impacts.

Australia has not yet experienced a malicious cyber incident causing catastrophic disruption to critical services. Over the last year, cyber incidents have increased with approximately 600 million attacks globally each day, according to Microsoft reporting. Recent high-profile incidents in Australia have involved theft of personally identifiable information. In contrast, deliberate attacks on critical infrastructure, including power grid outages and disruptions to water systems in North America and Europe have demonstrated the compounding risk impacts when operational systems are targeted.

The high-level cyber capability of nation-states seen in 2024 with strategic targeting of entities across multiple sectors, according to the Australian Signals Directorate's Australian Cyber Security Centre, has persisted into 2025. Other industry sources indicate that in some cases, there has been up to three to four times the number of cyber attacks compared to previous years. Pre-positioning, where malicious actors secretly embed code in systems to gain persistent and ongoing access without detection, remains a significant threat. This risk is highlighted by attempts from threat actors, such as Salt Typhoon, to infiltrate communications sector equipment and access downstream customer devices.

Cyber incidents are costly, including to an organisation's reputation, with most impacted sectors reporting significant disruption and long timeframes for recovery. A disproportionate focus on mitigating high-volume, low-impact attacks can leave infrastructure operators under-prepared for a potentially catastrophic incident.

CI2 Third-party providers continue to be a principal vector for cyber intrusion.

External providers play a critical role in many organisations and reliance on their digital services is unavoidable in many areas of modern critical infrastructure operations.

In 2025, data breaches impacting multiple Australian critical infrastructure operators that exposed the personal data of millions of customers, were caused by cyber-attacks exploiting vulnerabilities in third-party platforms.

The security of critical infrastructure is only as strong as its weakest link. Many third-party providers have access to sensitive data and the technical knowledge of their clients' cyber environments; in some instances, they maintain network connections that can be exploited and leveraged for access. Over the last two years, cyber-attacks targeting and exploiting third-party providers doubled globally, accounting for nearly one-third of all attacks, according to multiple industry reports.

Critical infrastructure operators must ensure that any external parties with access to their data or systems meet cyber security standards that are at least as strong as their own. Third-party risk should be managed to a standard equal to, or higher than, that applied within the organisation.

CI3 Progressively interconnected operational systems are a concerning vulnerability for critical infrastructure.

Operational technology (OT) systems are a valuable target for both state-backed and financially-motivated threat actors. Volt Typhoon's strategy of pre-positioning on IT networks to enable lateral movement to OT assets and disrupt physical critical infrastructure processes has been followed by other state-linked attacks, such as Salt Typhoon, targeting US telecommunications providers. Ransomware incidents have also targeted OT, as demonstrated by attacks causing disruptions to water and power providers in the United States.

Upgrading and securing digital systems is crucial for critical infrastructure, because many legacy OT systems were not designed to withstand today's cyber threats. The widespread use of internet-of-things (IoT) devices, together with new AI based tools has made digital infrastructure more interconnected than ever.

While this interconnectedness can boost efficiency, it also demands a stronger understanding of how to manage varying risk priorities across different platforms. This is a challenge for risk management and regulation alike. If not properly understood and managed, growing interconnectivity will expose other critical assets to security vulnerabilities from other platform and systems.

CI4 Large-scale adoption of artificial intelligence brings prosperity while creating more risk.

Digital interconnectedness defines the modern world. It enables innovation, collaboration, and business growth, and we have become accustomed to optimisation. However, in our pursuit of optimisation we must also be mindful of change that exposes us to security risks.

The use of AI for preventative digital resilience is reducing costs for organisations. Ongoing advances in the capability of AI powered digital tools have created new opportunities to improve efficiency and streamline processes, including for cybersecurity. While AI-based tools can provide enhanced monitoring, detection, and analysis of threats to cyber environments, they can also magnify the capabilities of threat actors and increase the vulnerability of connected systems and information.

Malicious actors are expected to act quickly to exploit any vulnerabilities in AI-integrated systems. It is vital that critical infrastructure operators proactively manage both the opportunities and risks introduced by AI-enabled tools.

CI5 Long-term digital resilience requires more than just reliance on compliance as main line of cyber defence.

Critical infrastructure operators need to move beyond compliance-based models and adopt a holistic, risk-based approach to cybersecurity. Regulatory standards are essential in providing a consistent baseline, but they cannot represent the highest possible standard for every operator. Many operators already take cybersecurity seriously, yet relying solely on compliance risks creating a false sense of security.

As technology evolves, resilience is no longer just about having the resources to detect and recover from attacks. Truly resilient digital systems must also prevent incidents where possible and maintain robust continuity plans to ensure service delivery when cyberattacks occur.

Case Study

Converging risk factors leading to devastating outcomes

Adversaries pose an increasingly sophisticated threat to critical infrastructure and can exploit multiple vulnerabilities via multiple vectors simultaneously. In April 2025, UK-based retailer Marks & Spencer (M&S) experienced a significant cyber incident from converging vulnerabilities that disrupted retail services including online orders, deliveries and payments for its range of products including food and groceries.

An offshore third-party service provider was targeted with a social-engineering attack that compromised login details of employees with access to M&S' operational systems, including legacy systems with likely weaker security controls. The subsequent ransomware attack caused service outages online and in stores and forced the retailer and its suppliers to resort to manual order processes for several weeks. Overall, this resulted in a significant financial cost in the hundreds of millions.

Open-source reporting suggests the same threat actor was responsible for separate attacks against critical infrastructure in Australia. This incident also exploited vulnerabilities in third-party services, although impacts were limited to a data breach of customer information with no disruption to services.

CROSS-SECTOR RISK PRIORITISATION FOR CYBER / INFORMATION THREAT

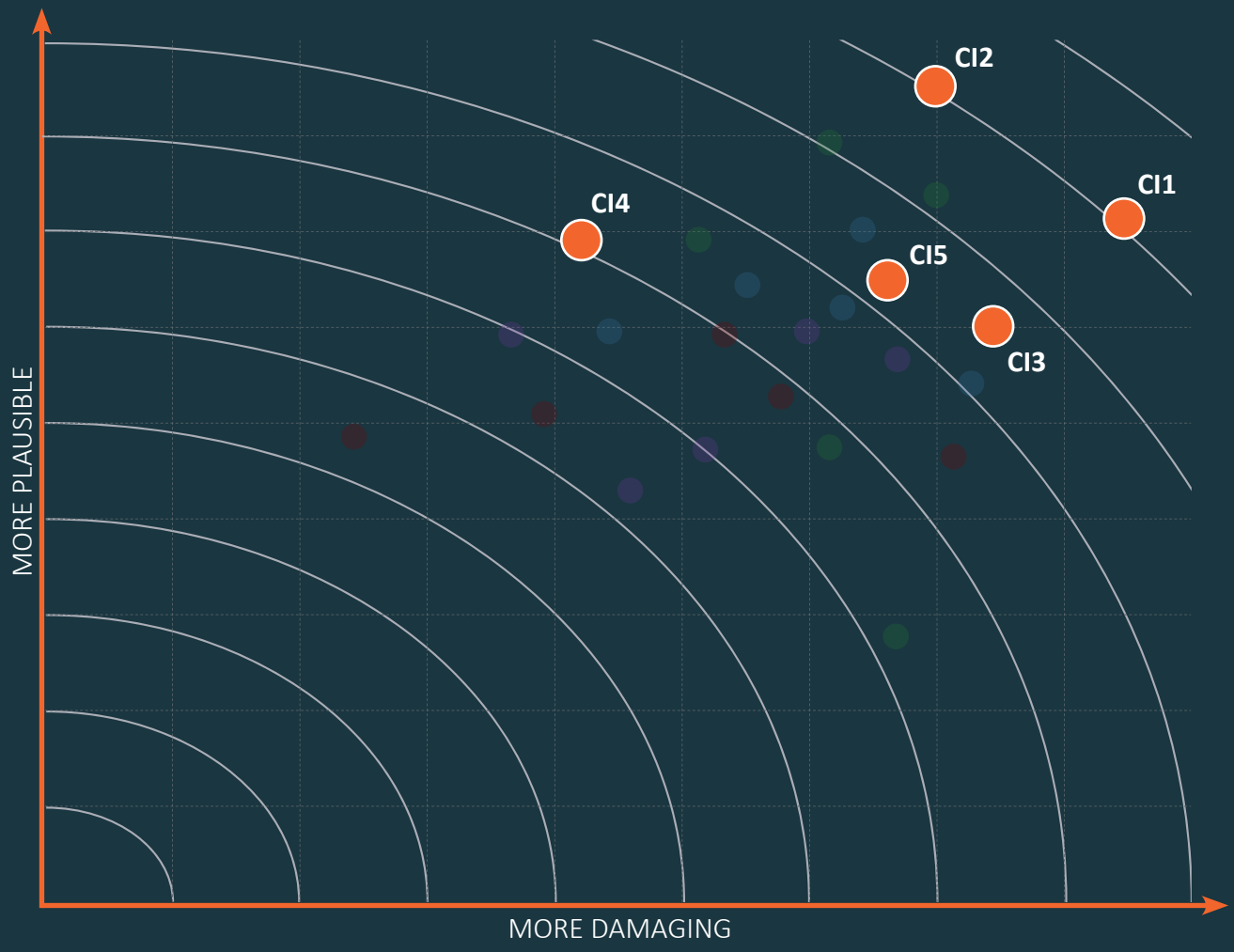


Figure 2. An illustration of cross-sector Cyber and Information risk prioritisation considering risk plausibility and damage.

- **CI1** Extreme-impact cyber incident
- **CI2** Third-party cyber risk
- **CI3** Risk from IT/OT/IoT connectivity
- **CI4** AI implementation risk
- **CI5** Limited levels of cyber security

Figure 2 highlights the Cyber/Information risk issues with a visual comparison of plausibility and damage. The comparative plotting was determined using structured qualitative analysis, drawing on CISC's understanding and ongoing assessment of critical infrastructure risks.

The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation specific to their own assets, operations and security measures.


SUPPLY CHAIN

Supply Chain

SC1 Physical supply chains have become more vulnerable than ever in the current global environment of uncertainty.

Australia's reliance on interconnected, international supply chains means we are over exposed to the potential impacts from offshore events. Geostrategic conflicts are not new, but greater uncertainty around geopolitical actions and market responses complicates short-term planning.

Uncertainty brings complexity for supply chain management, exacerbated by other factors including long distances from suppliers, a focus on just-in-time delivery models, and limited or no visibility of critical nodes within supply chains. All critical infrastructure sectors are reliant on international supply chains, with high dependence on the offshore manufacture of processed materials, technological components, chemicals and refined fuels, medicines, and fertilisers, among many other items.

It is vital that critical infrastructure operators clearly identify and monitor the supply chains that are essential to their business, so that associated risks can be managed and mitigated where possible. This includes developing robust business continuity and resilience mechanisms for when global conditions leave no choice but to endure the resulting supply shocks.

SC2 Obfuscation and lack of transparency heighten the risk from digital supply chains.

Digital services are an indispensable part of modern critical infrastructure operations, with secure access to software as essential as resilient supply chains for physical products. Different models, including software-as-a-service, cloud-based platforms, and outsourcing, can obscure the full range of service providers or the origins of their components. This can also conceal security vulnerabilities and the presence of malicious actors.

Critical infrastructure organisations often have limited choice of vendors and technology platforms, which means some risks are unavoidable. For example, many rely on major cloud providers, whose key functions (such as authentication services or storage redundancy) may be subcontracted offshore to jurisdictions with different privacy and security laws.

Incidents or technical outages experienced by service providers are not always disclosed to downstream customers, limiting critical infrastructure's ability to recognise, mitigate and manage operational risks.

SC3 Fuel security continues to be a high consequence concern for critical infrastructure operators.

Liquid fuel supply chains remain critical to the availability of services provided by all Australian critical infrastructure sectors. Even small disruptions to the availability of fuel in Australia can quickly cause cascading and disruptive impacts. Maintaining fuel supply resilience is essential and global fuel supply chain networks are highly sensitive to shocks and disruptions.

For critical infrastructure, fuel security extends well beyond the ability to refuel vehicles. Diesel is our most important and versatile fuel. It is vital for the onshore transportation of goods, food, equipment and medicines; it enables the functioning of emergency services; it provides critical redundancy for electricity generation for essential services including hospitals, water and sanitation, telecommunications infrastructure, and data centres. Aviation fuels are also essential; they enable deployment of critical workers, urgent delivery of medicines or critical components via air cargo, and the use of aircraft in a wide range of support roles such as surveying, surveillance and imagery collection.

In managing transition risk for net-zero and renewable energy sources across the economy, we must not lose sight of the potential impacts from disruption to liquid fuel supply chains and ensure these continue to be adequately managed.

SC4 Ongoing trends of less diversified supply sources is reducing resilience.

Limited diversification in the supply of critical components and materials places ongoing pressure on critical infrastructure sectors. A small number of countries and companies dominate production and processing, leaving supply chains exposed to disruption from geopolitical disputes, trade restrictions, natural disasters, foreign influence or other crises.

Market shifts, technology transitions and heavy reliance on single source or geographically clustered suppliers further increases vulnerability across the value chain, from raw material to distribution. For example, the declining number of onshore manufacturers for a range of critical chemicals has forced some infrastructure operators to pivot to offshore suppliers. This has caused short-term disruption during transition periods and introduced additional exposure to global supply hazards for operators involved in production of food and groceries, provision of healthcare, and in the water sector.

Continued resilience against supply chain impacts requires a focused and shared approach with partnership across government and industry. For effective risk management decision making, critical infrastructure operators need to understand potential supply disruption across the entire supply chain, and the likely impact each point will have on their access to resources.

SC5 Many critical infrastructure sectors still lack the required qualified and suitable personnel.

In 2025, training, capability and retention pathways continue to be insufficient to meet the demand for skilled and qualified technical personnel. Although this issue stretches across the economy, it is most acute for critical infrastructure operators in engineering and maintenance, cybersecurity, and the growing demand for changing skillsets in automation and implementation of AI-based solutions.

These ongoing staffing challenges undermine the resilience and operational reliability of essential services. The lack of specialised skills, at times combined with an ageing workforce, makes it difficult for operators to recruit and retain the talent necessary to manage complex networks and processes. This erodes the ability of operators to maintain, protect and modernise operational systems.

Without a sustained level of industry and government investment across all sectors in workforce development, training and retention strategies, multiple industries will continue to face compounding vulnerabilities. This will make it harder for critical infrastructure owners and operators to adapt to future demands and protect critical services from operational, technological and security risks.

Case Study

Dark clouds of conflict hang over global trade

In mid-2025, escalating tensions in the Middle East demonstrated how geopolitical shocks can reverberate through critical supply chains. Over 12 days, Israel, Iran and the United States engaged in direct military strikes. During the conflict, Iran's government actively considered closing the Strait of Hormuz, which is a chokepoint through which over 20% of global oil consumption flows.

Closure would have disrupted not only global energy markets, but also around 70% of Australia's urea imports, with flow-on effects for freight, agriculture and fuel security. Although quickly resolved, the event demonstrated the fragility of global supply routes and the speed with which international instability can disrupt essential sectors.

CROSS-SECTOR RISK PRIORITISATION FOR SUPPLY CHAIN HAZARD

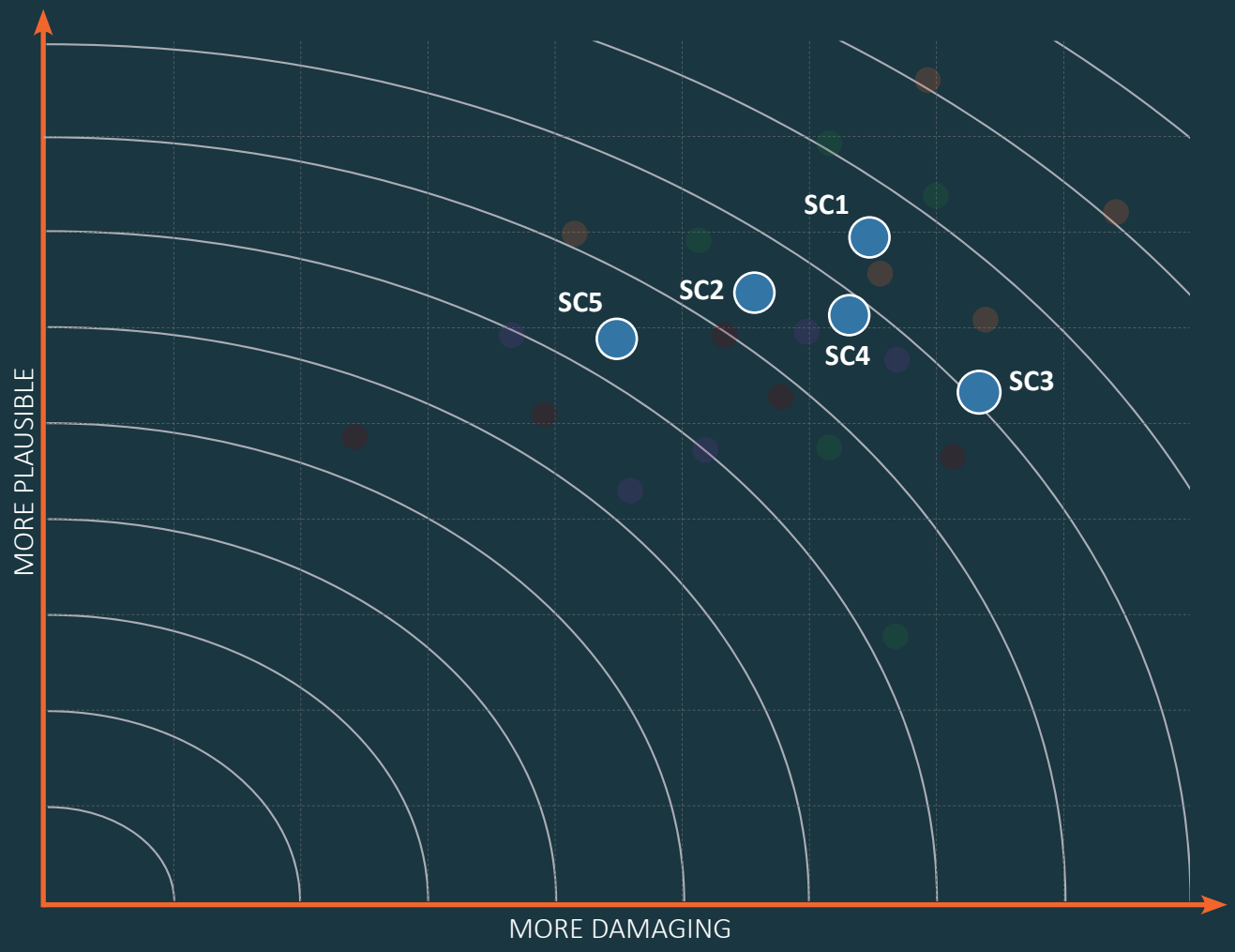


Figure 3. An illustration of cross-sector Supply Chain risk prioritisation considering risk plausibility and damage.

- **SC1** Geopolitically driven supply chain disruption
- **SC2** Digital supply chain risk
- **SC3** Disrupted fuel supply
- **SC4** Concentrated supply risk
- **SC5** Critical workforce and skills shortfalls

Figure 3 highlights the Supply Chain risk issues with a visual comparison of plausibility and damage. The comparative plotting was determined using structured qualitative analysis, drawing on CISC's understanding and ongoing assessment of critical infrastructure risks.

The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation specific to their own assets, operations and security measures.


PHYSICAL

Physical

PH1 **Sabotage to critical infrastructure has become a key tool for geopolitical disruption.**

Contemporary conflicts, such as Russia's invasion of Ukraine, have shown that physical sabotage to critical infrastructure is becoming a frontline weapon during periods of geostrategic conflict. In early 2025, Australia's Director-General of Security cautioned that sabotage is expected to pose an increasing threat in Australia over the next five years and the threshold for high-impact sabotage is closer.

Sabotage for geopolitical disruption will likely cause significant consequences, and our reliance on infrastructure and networks that extend beyond Australian territory and control increases our vulnerability to sabotage. Submarine cables carry 99% of Australia's international internet traffic though international waters; many sectors rely on services provided by space-based assets; and maritime and aviation supply lines facilitate our connection to the global economy.

Adversaries' exploitation of existing technologies, alongside emerging innovations, requires us to reshape the way we think about our exposure to sabotage risks. New submarine cable cutting devices are emerging with increased operational ranges. In 2025, Taiwan's submarine cables have been disrupted four times with two suspected incidents from vessel sabotage. Small uncrewed aircraft systems (UAS) are cheap and readily available and have been used with disruptive effect in the Russia-Ukraine conflict.

PH2 **Operational disruption from smaller, localised acts of sabotage should not be underestimated.**

Sabotage is not limited to large-scale, destructive attacks on physical infrastructure. It can also involve small-scale, selective and temporary acts of degradation, disruption or interference against networked infrastructure and physical systems.

Malign actors engage in disruptive behaviour for a variety of reasons. This includes financially-motived crime, single-issue or ideologically-driven protest, and chaotic or purposeless vandalism. When such actions target critical infrastructure, deliberately or inadvertently, they can cause localised sabotage and trigger cascading disruptions across interconnected networks.

Global incidents have demonstrated that small-scale, physical criminal acts can undermine operations nation-wide. This vulnerability is particularly acute when financially motivated actors target high-value assets within or connected to critical infrastructure. For example, theft of copper wiring has resulted in disruption to power supply across Australia, including recent outages in regional Queensland and metropolitan Perth. Overseas, the theft of signalling copper cables has disrupted passenger train services.

Ultimately, such acts demonstrate that the reliability of critical infrastructure depends increasingly on our ability to anticipate and mitigate local threats and vulnerabilities.

PH3 **The extremist threat from lone actors and small groups persists in its ability to create unpredictable outcomes for critical infrastructure security management.**

In the Australian security environment, violent extremists are likely to favour low-cost, locally-financed attacks using readily acquired weapons and simple tactics. Recent domestic incidents have highlighted that safeguarding critical infrastructure requires practical and effective physical security management.

In 2025, multiple airports suffered perimeter breaches from individuals who directly threatened the safety of flights and passengers. Arson has also been used in seemingly extremist tactics, including against businesses linked to Australia's defence industry.

Critical infrastructure requires robust security systems that can protect against both everyday disruptions and extreme events caused by individuals with malign intent. This may be achieved by balancing effectiveness for industry with efficiency, so procedures can accommodate a wide range of scenarios.

PH4 Grey zone tactics have the potential to interfere and influence the operation of Australian critical infrastructure.

The risks from grey zone tactics persist as a challenge in safeguarding Australia's critical infrastructure. Malicious actors can leverage ambiguity across jurisdictional security frameworks to conduct activities that are less obviously coercive than explicit military action. Regardless of whether this activity is deliberate or simply careless, it can still present a real physical hazard.

Over 2025, Australia's maritime environments have been exposed as vulnerable to grey zone activity. Foreign research vessels purportedly conducting scientific missions have circumnavigated Australia's exclusive economic zone in proximity to seabed cables and maritime routes. Meanwhile, vessels from the People's Liberation Army-Navy conducted live fire exercises in international waters off Australia's east coast, endangering the physical safety of aviation and maritime transport.

Although ill-intent in incidents such as these may be plausibly deniable, the resulting disruption to infrastructure is a real impact that must be recognised, anticipated, and managed where possible.

PH5 High-risk and single-source vendors are creating risk from counterproductive foreign influence over critical infrastructure.

Reliance on high-risk, concentrated and single-source vendors can introduce significant physical security vulnerabilities within Australia's critical infrastructure. Vendors operating under foreign jurisdictions may be subject to laws compelling cooperation with state-based threat actors, increasing exposure to foreign influence and exacerbating the risk of foreign interference.

Vendors of key components and services often have physical access to infrastructure facilities, enabling the potential installation of unauthorised hardware components, including covert monitoring devices or backdoors. These devices could facilitate unauthorised, remote control over critical systems, disrupting asset operation and causing cascading disruption across the sector.

A German defence ministry-commissioned report warned that foreign-manufactured wind turbines could be exploited to delay projects, harvest sensitive data or remotely disable turbines to leverage energy infrastructure for political coercion. Similarly, United States officials discovered hidden communication modules in foreign-made solar inverters that could allow external actors to disrupt power grid operations, raising alarm about the security of renewable energy systems. Rigorous vendor assessments should be undertaken and stringent technical controls and governance arrangements implemented to safeguard Australia's critical infrastructure from such activity.

Case Study

Overseas conflict heats up security risks for Australia

In late 2024, a campaign of physical sabotage impacted interconnected global critical infrastructure, forcing industry and the Australian Government to respond. State-linked Russian threat actors concealed incendiary devices in international air cargo to target countries providing support to Ukraine. Disruption from the attack was initially limited to fires at freight facilities in Germany and the United Kingdom. However, due to the international nature of global air freight it was quickly identified that other countries including Australia could be affected, both deliberately and inadvertently.

To protect freight systems and ensure the safety of the public, the Department of Home Affairs issued a Special Security Direction under the *Aviation Transport Security Act 2004*. This introduced security measures to reduce exposure to the sabotage threat, and to detect potential attempts to target the Australian transport sector. This incident highlights how state actors may deliberately use physical sabotage as a political tool during times of heightened tension. Australia is not immune from the potential consequences.

CROSS-SECTOR RISK PRIORITISATION FOR PHYSICAL THREAT

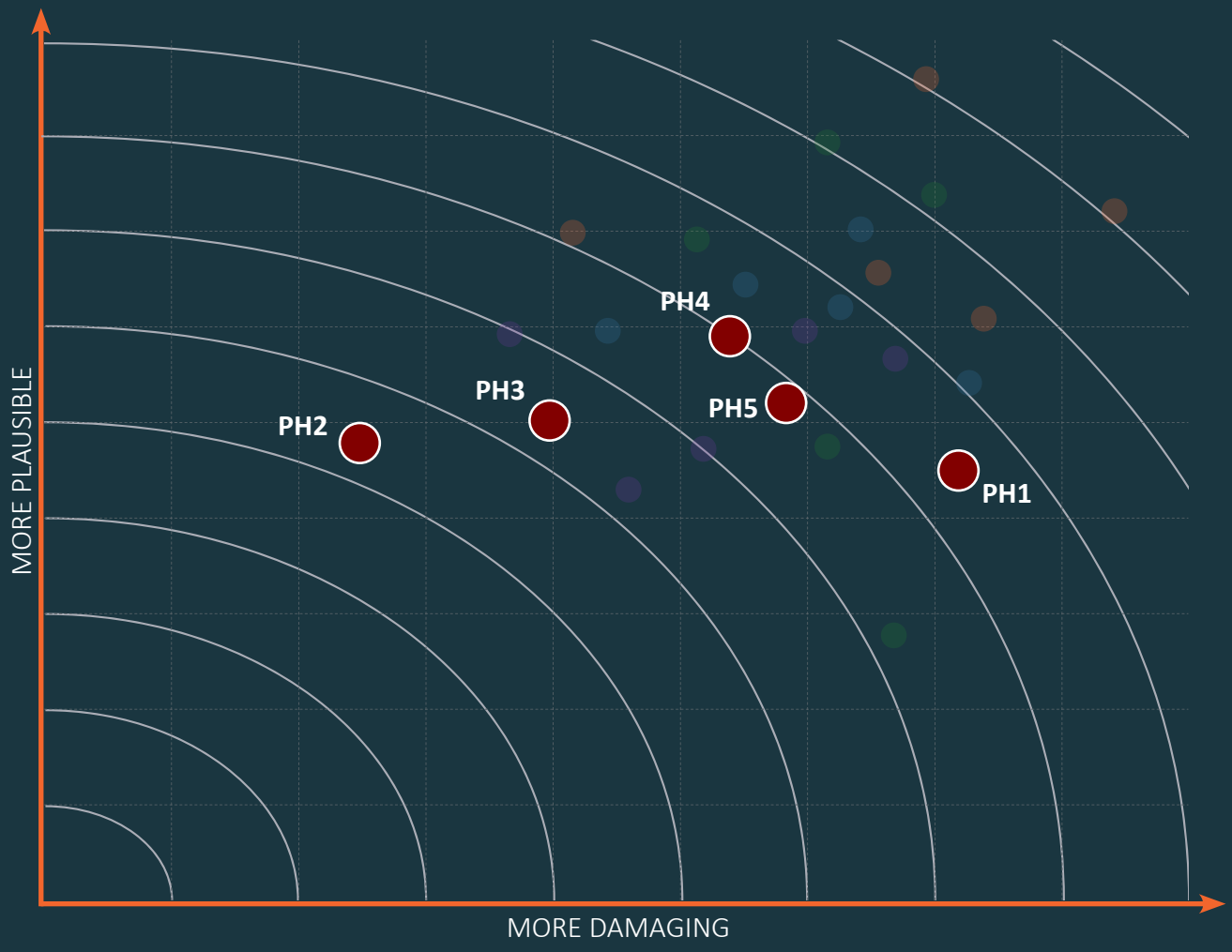


Figure 4. An illustration of cross-sector Physical risk prioritisation considering risk plausibility and damage.

- **PH1** State-sponsored sabotage
- **PH2** Issue-motivated and criminal sabotage
- **PH3** Lone actor extremism
- **PH4** Grey zone disruption
- **PH5** Foreign interference risk

Figure 4 highlights the Physical risk issues with a visual comparison of plausibility and damage. The comparative plotting was determined using structured qualitative analysis, drawing on CISC's understanding and ongoing assessment of critical infrastructure risks.

The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation specific to their own assets, operations and security measures.


NATURAL HAZARD

Natural Hazard

NH1 Severe weather events are occurring in unexpected areas with unexpected frequency.

Climate change is altering the geographical distribution of risk, exposing new geographic areas to more frequent and severe weather events. Australia is accustomed to the impact of storms, floods and bushfires. However, as severe weather moves beyond historically affected regions, it may exceed safety and construction standards that were designed for different conditions.

Population growth is extending development into hazard-prone areas, increasing exposure to high winds, flooding and bushfires. Ex-Tropical Cyclone Alfred posed a significant risk to Brisbane and while the city was spared from the most severe impacts, cascading disruption across multiple critical infrastructure sectors still affected supply chains, transport, water and power. Internationally, the Los Angeles wildfires illustrated the severe consequences that arise when local environments and infrastructure are highly exposed to natural hazards.

Australia's critical infrastructure is more extensive, expensive and interconnected than ever; it also contains ageing components or assets engineered for an environment unaccustomed to certain levels of hazards. Whole-of-system resilience depends on planning for changing hazard exposure and accounting for the potential impact of infrequent but high consequence events.

NH2 Recovery periods between natural disaster events are contracting.

Historical patterns are not the best guide for developing natural hazard resilience and recovery plans. Severe weather events, and how they impact our infrastructure, are becoming harder to predict. Disasters have struck adjacent areas simultaneously or have hit the same locality in quick succession, causing 'climate whiplash' as sharp swings between extreme wet and dry conditions exacerbate the impact of subsequent weather events.

Local resources for response and recovery can be insufficient for concurrent or consecutive crises, leaving communities and infrastructure underprepared when a disaster strikes. Constrained local, state and federal government budgets are squeezed to restore priority infrastructure assets, leading to lagging repairs on non-priority assets resulting in longer replacement and repair timeframes.

NH3 Critical infrastructure planning may not be prioritising preparation for natural hazard extremes in a changed climate.

Australian operators are experienced in managing the impacts of frequently occurring natural hazards. However, infrastructure networks are becoming more extensive, in some cases more exposed to hazards, and more expensive to repair. Resilience planning must consider both the potential financial impacts of natural hazards and the inherent vulnerabilities that make systems more susceptible to damage from extreme events.

Due to the complexity of global weather patterns and natural variability, the exact effect of changes in the climate are hard to pinpoint. Research indicates that extreme temperature events and heatwaves are likely to increase, and storm events with high winds and rain likely to impact critical infrastructure may increase in intensity. As infrastructure networks expand to support increasing demand, so too the potential cost from a severe event impacting those networks.

It is vital that changes in extreme weather are evaluated as part of planning and development, so that infrastructure systems are resilient to the future hazard environment. Cooperation and coordination nationally can assist in identifying and implementing cross-sectoral or jurisdictional responses to systemic barriers.

NH4 Solar storm activity over the last 12 months has exposed the susceptibility of critical infrastructure and its dependencies to low probability, high impact events.

Awareness of space weather and its potential effects has grown in the past two decades. However, comprehensive understanding of the risk to critical infrastructure remains challenging. The risk presented by extreme space weather remains both significant and obscure; it is a complex hazard with potentially significant consequences for critical infrastructure. With our increasing reliance on technology, extreme space weather has the potential to disrupt many of Australia's critical services.

The potential impact extreme space weather could have on modern critical infrastructure, society and the economy, while widely acknowledged, remains uncertain and untested. In May 2025, X-ray and ultraviolet radiation from a series of solar flares impacted the Earth's atmosphere, affecting Europe, Asia, the Middle East, and North and South America. This blocked high frequency radio signals, impacted power grids and disrupted positioning, navigation and timing (PNT) systems.

Much of our modern technology has yet to experience a direct, extreme space weather event. Furthermore, growing interdependency between our critical infrastructure sectors has created an environment where any direct effects on one sector can easily extend the impacts across sectors.

NH5 Almost all natural hazard events have cascading impacts due to interconnected critical infrastructure.

Our critical infrastructure is deeply interconnected. Significant disruption in one sector will affect others, and cascading effects from a natural hazard incident on critical operations needs to be distinguished and analysed as part of risk assessments. Impacts from extreme hazards are easily magnified by 'creeping dependency', the gradual growth of interdependent critical infrastructure systems over time.

The complex relationships between cross-dependent sectors need to be clearly understood by asset holders and government, mapped effectively, strengthened and managed so that function, effectiveness, safety and resilience are built into all critical infrastructure environments.

All sectors should consider recovery response times impacted by supply chain cuts; staffing shortages; damage from multiple events; service disruptions; accessibility during an event; essential supplies and the ability to meet emergency demands; economic impacts from shortages or lack of supplies.

Case Study

From small things, big things grow

In late 2024, severe weather damaged transmission lines that supplied power to a regional NSW town. Less than a week later, the generator used for backup power supply overheated and tripped, resulting in ongoing power outages to residents and critical services. This extended the consequences for the community beyond those of the initial severe weather event itself.

From a single impacted sector, extended consequences from the incidents highlight our exposed interdependent infrastructure. Phone and internet services were halted; pharmacy cold storage was disrupted, damaging stockholdings of sensitive medicines; and a food and grocery businesses were also impacted. Access to transport fuels became limited, with not all petrol stations able to operate equipment.

Although occurring at a regional level, it demonstrates the close interconnection of our critical services and how cascading effects can cause disruption much wider than the initial hazard impact.

CROSS-SECTOR RISK PRIORITISATION FOR NATURAL HAZARDS

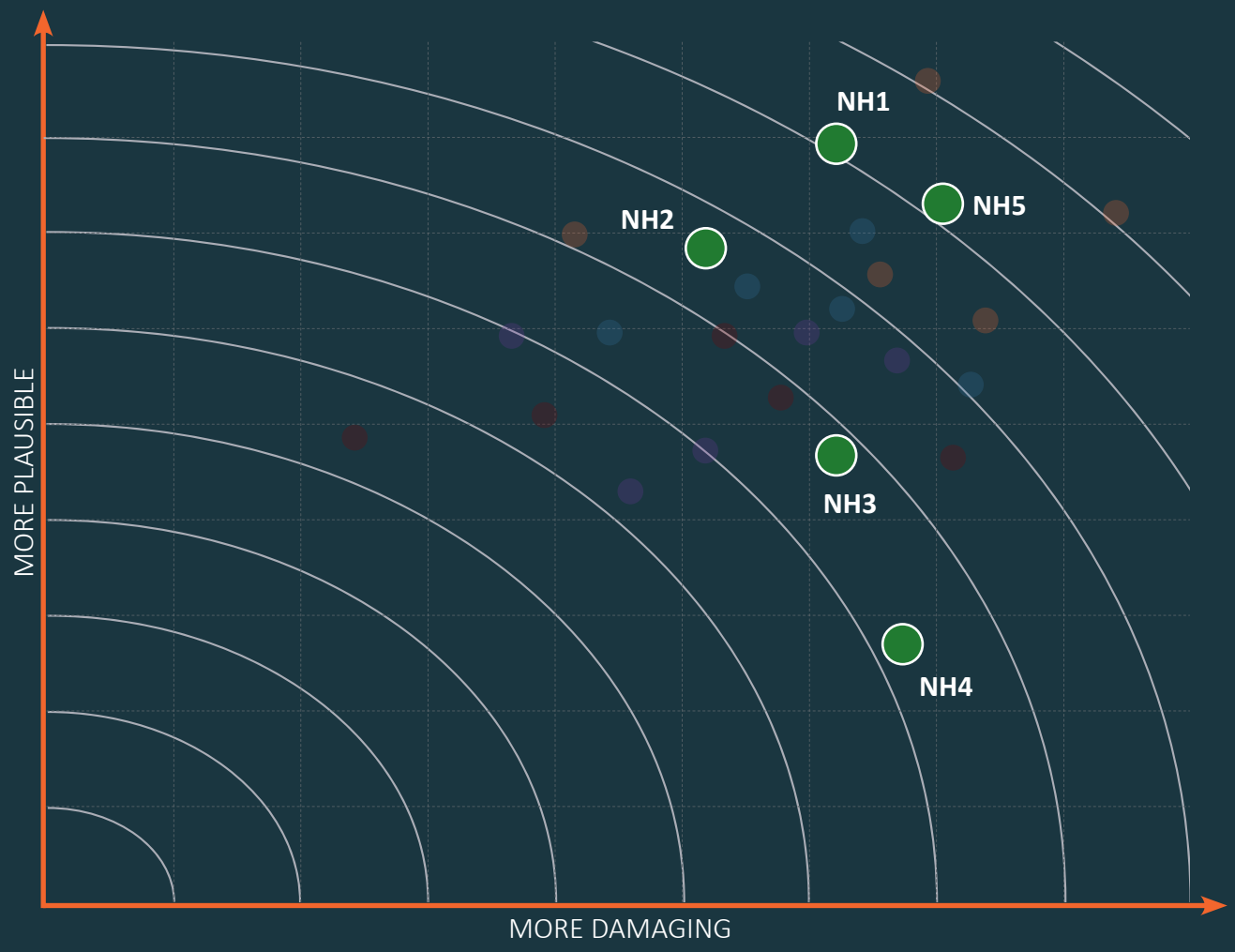


Figure 5. An illustration of cross-sector Natural Hazard risk prioritisation considering risk plausibility and damage.

- **NH1** Unexpected severe weather location and frequency
- **NH2** Reduced natural hazard recovery opportunity
- **NH3** Unpreparedness for future extreme weather
- **NH4** Extreme space weather event
- **NH5** Significant disruption from interdependent infrastructure

Figure 5 highlights the Natural Hazard risk issues with a visual comparison of plausibility and damage. The comparative plotting was determined using structured qualitative analysis, drawing on CISC's understanding and ongoing assessment of critical infrastructure risks.

The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation specific to their own assets, operations and security measures.


PERSONNEL

Personnel

PE1 Damaging consequences for critical infrastructure from accidental incidents remain a concerning risk.

Human error is ubiquitous. Over the last 12 months, some of the most notable disruptions to critical infrastructure have been caused by human error or compromised/faulty system updates inadvertently deployed to operators at scale. Despite the development and hardening of response mechanisms, responsible entities for critical infrastructure are not immune to accidental incidents, whether internal or external to the business that can have significant impacts.

Impacts from accidental incidents in Australia have included disruption to communication networks, including to triple-zero services, delays to rail and aviation services, healthcare providers unable to collect patient data, and customers being unable to use payment systems. A deeply interconnected network of service providers across critical infrastructure means that incidents within one organisation, even if they are accidental in nature, may have cascading impacts to other connected entities and services.

An awareness of the potential consequences of accepted risks, and a willingness to address shortcomings, has never been more crucial in mitigating accidental incidents. The most sophisticated risk management plan may be completely undermined by an accidental incident from within.

PE2 Contracted workforces are a critical vulnerability for exploiting insider access.

Temporary, contractual, and externally-provided staff who do not undergo the same vetting processes and security training as permanent employees often pose a higher security risk. Contractors are often afforded trusted and privileged access to critical infrastructure information, systems or networks, which can make them an attractive target for exploitation. Malicious actors seeking to cultivate an insider may exploit high levels of contractor mobility and reduced workplace oversight.

Host organisations have limited control over how potentially sensitive retained information is used or secured once a contracted worker leaves the host workplace. The effectiveness of traditional personnel security mechanisms, designed to mitigate insider threats within a permanent, in-house workforce, is then limited.

Critical infrastructure entities should ensure personnel security measures appropriately address potential security vulnerabilities when engaging contractors. Thorough background and reference checks on contracted services remains an enduring mitigation, but other measures include restricting staff access, engaging least-privilege principles, and logging, monitoring and auditing contracted staff activities regularly to quickly detect any malicious activity.

PE3 Critical capability assurance and redundancy requires high priority alongside increases in automation.

Challenges persist in attracting, developing, and retaining skilled workforces. This is exacerbated by the emergence of new skillsets, an ageing workforce, and shortages in critical technical and professional roles. When combined with increased adoption of technologies such as AI and automation, there are several risks that must be considered.

Generative AI can hallucinate, where it presents inaccurate or misleading information as fact. Automation tools may be unable to consider nuance and broader operational context that is otherwise apparent to a skilled and experienced human worker. Without appropriate oversight and assurance, reliance on these systems may result in critical errors going undetected. For critical infrastructure, consequences could range from sub-optimal performance to critical system failure. An over-reliance on AI and automation could lead to the degradation of individual skills and capabilities, and a loss of business-critical corporate knowledge. Should automation technologies fail at a critical time, what may have been a manageable incident may rapidly escalate out of control without appropriately trained personnel.

Human oversight over decision making and evaluation functions will help to reduce risks when utilising these evolving technologies. Despite the efficiencies of automation, ensuring skillset capability and redundancy is maintained, in the event of technology failure, remains vital for business continuity planning.

PE4 Workforce upskilling is not keeping pace with requirements of the next generational security environment.

As the digital environment changes, and society's reliance on technology and connectivity grows, we must be prepared to address the security challenges that result. Investment to develop security literacy, capability and expertise of critical personnel is required to manage ubiquitous AI tools, strengthen the security culture required to fend off espionage and foreign interference, and prepare for a post-quantum encryption environment.

Australians are implementing AI in their workplaces without robust training and guardrails in place to ensure a responsible use of AI. In a global research study, approximately half of surveyed Australians reported they had uploaded sensitive company data, such as client data or financial records, into publicly accessible tools AI tools. Irresponsible or uninformed use of AI can inadvertently create exposure to state-sponsored espionage and cyber threats.

To address these risks, critical infrastructure can implement AI strategies, accompanied with policies and procedures, governing its responsible use in the workplace.

Investing in AI literacy training to ensure responsible use by employees can further protect entities as the pace of technological change increases.

PE5 Interaction with more sophisticated deepfake technology is challenging the ability to determine friend from foe.

Deepfake technology enables the creation of hyper-realistic videos and voice clones that are nearly indistinguishable from genuine humans. Malicious actors have used deepfake technology to impersonate trusted personnel in real-time, bypass regular authentication requirements, and extract financial gain or obtain access to IT networks.

As this technology grows increasingly sophisticated and harder to detect, staff face increasing pressure to withstand convincing social engineering attacks. Deepfakes are one of the many capabilities of generative AI that exacerbate the already challenging environment of misinformation and disinformation. Collectively, these tools can be used as part of a campaign to cultivate a potential insider for malicious activity, or to leverage an unwitting insider to grant an unauthorised user access to sensitive information, or even operational control over assets.

Currently, leading deepfake detectors are unable to identify real-world deepfakes reliably, according to CSIRO research. As the arms race between AI-powered threats and threat detection continues, it is important that critical infrastructure entities equip their staff to mitigate these risks as part of security culture and awareness training.

Case Study

Virtual wolves in sheep's clothing

In 2025, the use of deepfakes has become more daring and audacious. State-sponsored threat actors leveraged Deepfakes in multiple attempts to establish and exploit personnel security vulnerabilities and then gain systems access. In one incident, deepfake personas consisting of a collection of images and video footage were used to apply for remote-worker IT and cyber security roles. In another, threat actors sent an employee a link to a video meeting with deepfake impersonations of their own senior leadership and other stakeholders. The employee was then directed to download an extension for the video meeting. In both cases, deepfakes enabled the threat actors to build trust with unwitting insiders and allowed them to bypass security measures, gain system access and install malware.

These incidents show the evolving threat capabilities that can be used to target insiders and also highlight the personnel security risks that can be associated with offshore or contracted workers, and the need for an uplift in organisational security culture to recognise and mitigate these risks.

CROSS-SECTOR RISK PRIORITISATION FOR PERSONNEL THREAT

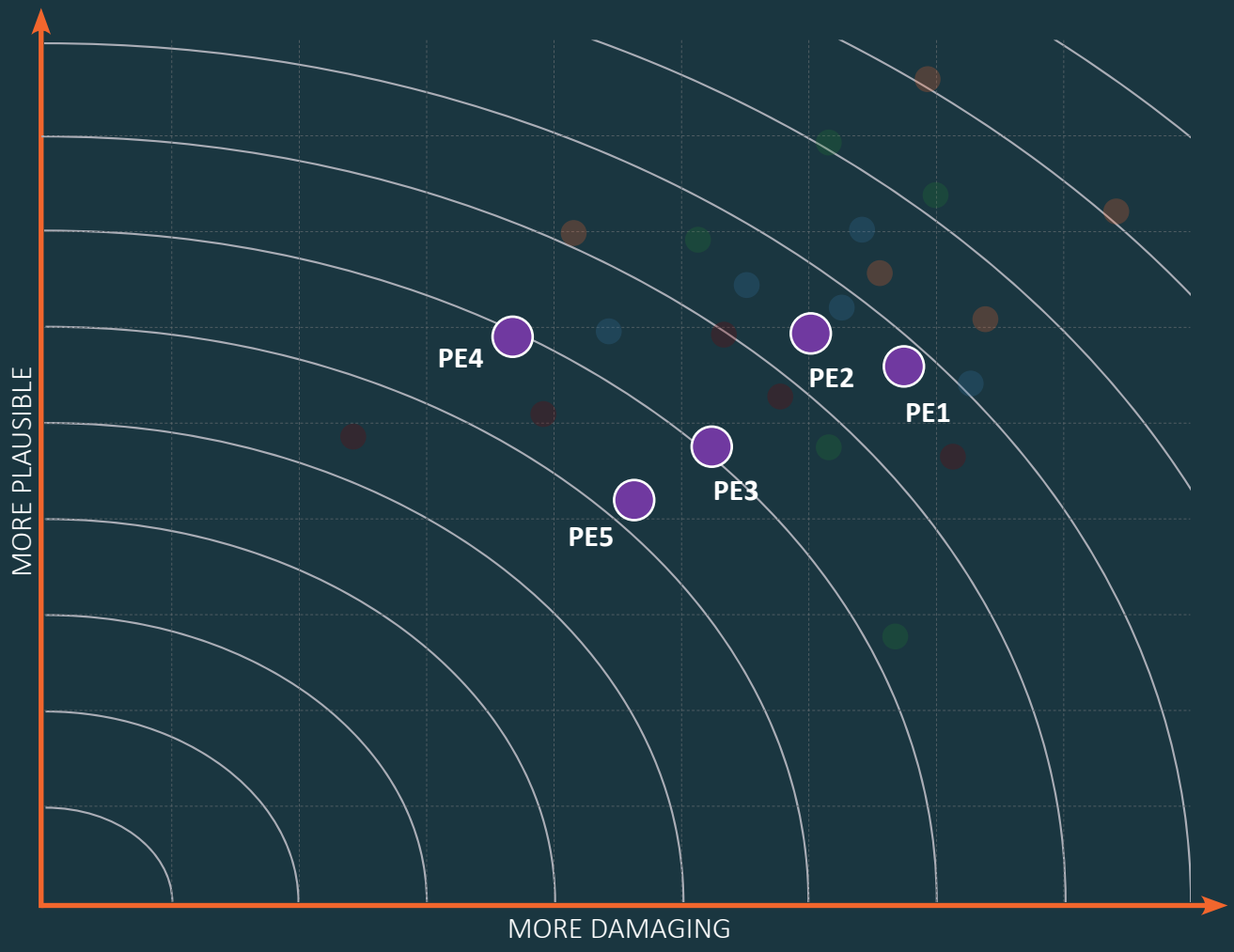


Figure 6. An illustration of cross-sector Personnel risk prioritisation considering risk plausibility and damage.

- **PE1** Insider-initiated capability outage
- **PE2** Contracted workforce insider risk
- **PE3** Misaligned workforce/automation balance
- **PE4** Workforce critical skill gaps
- **PE5** AI-augmented social engineering attacks

Figure 6 highlights the Personnel risk issues with a visual comparison of plausibility and damage. The comparative plotting was determined using structured qualitative analysis, drawing on CISC's understanding and ongoing assessment of critical infrastructure risks.

The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation specific to their own assets, operations and security measures.


LOOKING AHEAD

Looking Ahead

Technology trends and risk drivers intersect in complex and sometimes unpredictable ways, making it difficult to anticipate their full impact across critical infrastructure sectors.

The following are a selection of drivers identified by CISC that are likely to shape Australia's critical infrastructure security risk profile in coming years.

An inability to shift from single-source or geographically concentrated suppliers will lead to more disruptive impacts.

The supplier landscape is shifting in response to commercial, regulatory and other pressures. In some sectors, this is trending towards fewer suppliers with greater geographic concentration, exposing critical infrastructure to risks from unexpected or unpredictable decisions from foreign governments, companies and intermediaries. Geographic concentration also creates risk when economic or political priorities are inconsistent with Australia's interests.

Changes in risk appetite, or in preferential supply arrangements by owners, suppliers or government may require Australian businesses to adapt to maintain service delivery. These changes are not always transparent, and adaptation is unlikely to be rapid or straightforward.

Resilience is likely be reduced where key suppliers operate in an environment of potential political interference, or where particular suppliers dominate the market. Unpredictable and sudden cessation of key products and services may be a feature of future operating environments, and supply chain resilience is likely to decrease as a result. Private commercial entities may vary the provision or availability of their key services for a variety of reasons, including for commercial, ideological and political outcomes.

The possibility of conflict in our region continues to loom as a key risk for assured delivery of our critical infrastructure.

Geopolitical uncertainty creates difficulty for industry and government in anticipating and planning for potential major armed conflict in our region. Conflict in locations where we have a high supply chain dependence, or those involving major powers, could escalate quickly and create immediate consequences for our critical infrastructure, particularly in the transportation and communication sectors.

Ongoing attacks on shipping in the Red Sea have highlighted how the targeting of key supply lines can cause significant disruption to global shipping. Similar events in our region could create even more severe disruption to transportation or completely cut off our access to critical supplies.

Indirect targeting of Australian critical infrastructure will remain a risk regardless of our level of involvement in any future conflict. Direct attacks exploiting pre-positioned cyber or personnel threats may be initiated with unpredictable consequences. Unattributable or plausibly deniable sabotage against critical infrastructure by nation-states may escalate in times of heightened geopolitical instability. Fractures in our social cohesion may also be exacerbated during conflict, which could result in disruptive activity against critical infrastructure.

Risks from sabotage against critical infrastructure are unlikely to ease with current trends in geopolitics and global social cohesion.

International and domestic issues are stirring discontent and disagreement, and adversaries are growing more willing to disrupt or destroy critical infrastructure as a response. Australia's Director-General of Security has stated Australia can expect foreign regimes to pre position with cyber access vectors, and that we are moving closer to the threshold for high-impact sabotage.

Radicalisation has also become unpredictable and issue-motivated disruption is becoming more concerning; both can be triggered by global issues. Critical infrastructure is a potential target for a lone-actor violent extremist, or for larger-scale ideological sabotage and disruption.

Sabotage targeting Australian assets directly or targeting international infrastructure or suppliers relied on by Australian critical infrastructure, could cause significant disruption to our ability to provide domestic services.

Agentic artificial intelligence will introduce new and more complex risks.

The implementation of agentic AI in the operation of critical infrastructure and upstream component services may have unexpected and disruptive results. This will be exacerbated in complex systems, where outcomes are difficult to map out or predict and where AI agents interact with each other. When AI is used for operational decisions, we may see major unexpected system behaviour.

A growing use of AI is inevitable, and this is occurring in the context of increasingly complex and interconnected critical infrastructure. AI has had a rapid uptake in most businesses in recent years. There is already recognition of the value of agentic AI, where it is used to make decisions within a specified operating context. Agentic AI has potential for use in a variety of applications from customer service to optimisation of complex networks.

Critical infrastructure owners and operators will aim to introduce AI tools responsibly. However, some AI-produced decisions continue to surprise researchers, and agentic AI will not always mirror human decision-making. If AI-tools make unpredictable and unexpected decisions that would not be made by a trained human operator, otherwise small disruptions in complex operational systems could cascade or compound.

Reliance on space-based technology will peak for the operation of most critical infrastructure sectors.

The dual-use capabilities of space technology have already extended geostrategic concerns and dynamics into space.

The growth of the space economy has also resulted in the private sector controlling a large portion of space-based assets, most significantly in low earth orbit. Private, corporate and government customers have shown a readiness to adopt space-based communications services like Starlink. With several competing satellite constellations entering the market, these are likely to become even more competitive with terrestrial services.

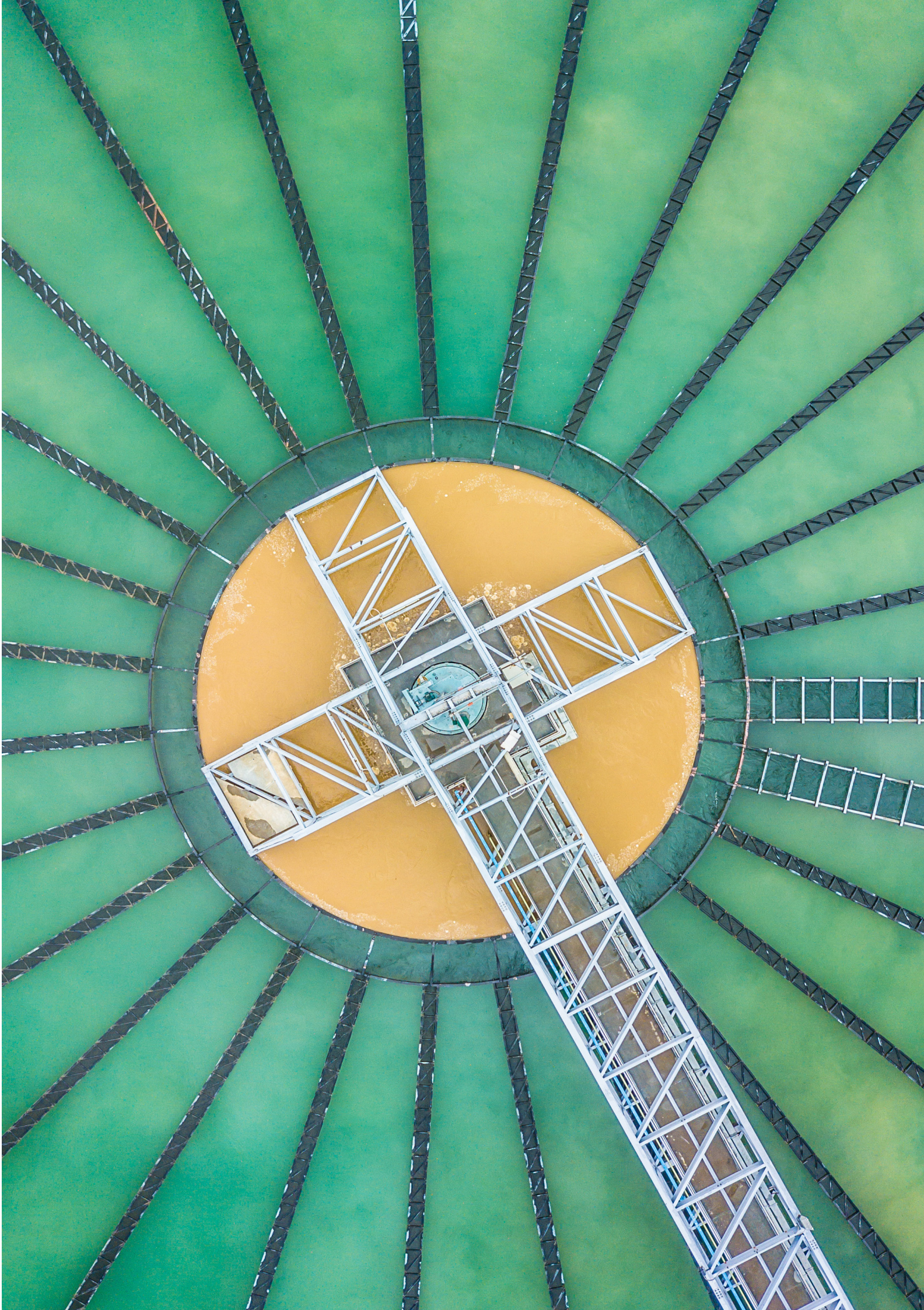
Most critical infrastructure sectors have space-dependencies, including positioning, navigation and timing, and communications. Satellite communication and space-generated data enables more than half of the critical infrastructure of advanced economies, according to the Organisation for Economic Cooperation and Development. As this dependence increases, the risk of more significant disruption across other critical infrastructure, from the failure or cessation of space-based services, will rise.

Space-based assets remain vulnerable to a wide variety of threats and hazards; attributing cause to any disruption can be difficult. Timeframes for recovery where there has been catastrophic failure or disruption to space assets is often lengthy due to challenges in sustaining the space environment.

Transitioning to post-quantum cryptography standards requires an invested and timely start.

The future of quantum technologies offers both opportunity and risk in advancing computing capabilities. From improving sensor abilities, to optimising logistics and planning or enhancing communications security, both critical infrastructure operators and government must remain diligent in preparing for the changes this technology is expected to bring.

The forecast capabilities of fault-tolerant quantum computers will undermine the cryptographic standards currently relied on for communications and cybersecurity, rendering current security measures redundant. Developing and implementing transition plans that assess vulnerabilities across data holdings, large legacy systems and current cybersecurity protocols is a large task, but necessary for critical infrastructure to meet an approaching deadline of operationalised quantum computing.



Australian Government

Department of Home Affairs

CRITICAL
INFRASTRUCTURE SECURITY
CENTRE