Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE



Critical Infrastructure Annual Risk Review

Fourth Edition
November 2026

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

This means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Contact us

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

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

Contents

2 Foreword

3 About the Critical Infrastructure Security Centre

4 Introduction

6 Risk Trends and Prioritisation

8 AI Dependencies and Effects

10 Cyber / Information

14 Supply Chain

18 Physical

22 Natural Hazard

26 Personnel

30 Looking Ahead

Foreword



Protecting Australia's critical infrastructure is essential to our security and prosperity.

The Australian Government's 2026 Critical Infrastructure Annual Risk Review provides a strategic overview of the risks to Australia's critical infrastructure and their impact on operational delivery. It draws on information provided to the Department of Home Affairs by Australia's critical infrastructure owners and operators, from Government agencies and the National Intelligence Community.

The Annual Risk Review is designed to help owners and operators of critical infrastructure better understand and respond to a wide range of risks. These include cyber threats supercharged by AI, the malicious use of emerging technologies, physical and human security threats, supply chain weaknesses, natural disasters and the increasing effects of climate change.

Attentiveness, proactive governance and informed leadership will be essential to ensure the resilience of Australia's critical infrastructure and the communities it services, along with the economy and national security it relies on.

Our critical infrastructure is under constant threat in a dynamic, diverse and degraded security environment. Rapid advances in artificial intelligence, automation, digital connectivity and other new technologies are improving how essential services are delivered, but they can also introduce or extend vulnerabilities that can lead to service disruption and potentially exploitation of Australians' information.

While more Australian organisations are adopting AI systems and digital platforms to drive greater efficiency, innovation and productivity, it's also important to understand how the risks they bring are interconnected. The Australian Government is working with technical experts and international partners to improve cybersecurity across the economy and strengthen the protection of key sectors, including energy, water, healthcare, transport and communications.

The Australian Government and the Department of Home Affairs remain committed to providing clear, practical guidance to help critical infrastructure operators manage these risks, understand their regulatory responsibilities and protect the systems and assets that support Australia's economy and national resilience.



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 to deliver 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 assessments 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. Our regulatory approach seeks to help industry understand that compliance is not just a matter of legal obligation, but integral to protecting the essential services all Australians rely on. The following five regulatory principles inform us in exercising our regulatory activities to achieve positive security outcomes:

1. Focus on risk and positive outcomes.
2. Promote voluntary compliance.
3. Be accountable, fair, and transparent.
4. Consistency and predictability.
5. Proportionate decision-making.

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 Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (Enhanced CIRMP Rules) builds on the baseline requirements.
- The Critical Infrastructure Risk Management Plan (CIRMP) Guidance provides plain language interpretation and best practice approaches to compliance with CIRMP obligations.
- The Foreign Ownership, Control, or Influence Risk Assessment Guidance and model contract clauses help to manage potential risk posed by vendors operating in supply chains.
- The Horizon 2 (2026-28) component of the Australian Cyber Security Strategy aims to strengthen cyber maturity across Australia, protect critical infrastructure and government systems, and secure digital technology.

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

Introduction

The fourth 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 2026.

Risk issues are presented for the five hazard categories: cyber and information security; supply chain; physical security; natural hazard; and personnel security. These categories are detailed in the *Security of Critical Infrastructure Act 2018* (SOCI Act) and accompanying rules for CIRMPs and are further defined below.

The brave new world of artificial intelligence

For over a decade, the arrival of artificial intelligence (AI) as a mainstay of critical infrastructure operations has been on the horizon, a transformative evolution many anticipated and now is embedded into our world. That future is no longer approaching, it has arrived.

Over the past 12 months, AI has integrated into operations at a pace that will reshape how critical infrastructure is designed, managed and protected. As AI becomes embedded in decision-making, automation, security and service delivery, its influence is expanding across every hazard category, creating new pathways for both risk and resilience.

This is a defining moment facing critical infrastructure operators. The challenge is how organisations will harness the opportunities, confront the threats that emerge, and establish governance frameworks capable of managing an increasingly complex risk landscape.

Decisions made today will help ensure that AI becomes a force multiplier for security and not an uncontrolled source of vulnerabilities.

The 2026 Critical Infrastructure Annual Risk Review highlights the growing reach of AI-driven risks across the full spectrum of hazards.

Cyber vulnerabilities are being rapidly uncovered by AI and will require AI-enabled mitigation strategies as the threat environment is continually reshaped by new technologies.

Risk in digital **supply chains** is mounting with reliance on AI tools for software and the rapidly transforming demand for hardware to supply AI capabilities.

Physical security requirements for infrastructure underpinning AI and connected technologies used across infrastructure assets are at the forefront of resilience challenges.

AI-fuelled mis- and dis-information is contributing to declining public trust in government and critical infrastructure operators, including when responding to **natural hazards** when communites are often at their most vulnerable.

Governance providing guardrails for implementation of AI tools in critical infrastructure operations is now a key **personnel** security risk mitigation requirement.

A period of global polycrisis

The risk environment facing Australia's critical infrastructure is shifting from complicated to complex. Geopolitical tensions are reshaping global power dynamics; conflict, grey zone activity and trade disputes are disrupting supply chains; and technology is rewiring the global economy. Critical infrastructure operators now face multiple global crises that are having significant impacts on how critical services are delivered and how risks to those services are managed. These separate crises are exacerbating and reshaping one another.

Polycrisis is an entanglement of crises across different global systems, including climate change, regional conflicts, supply chain disruption, and emerging biohazards. Each are significant in scope, damaging in cascading effects and challenging to predict, manage and understand.

Intertwined crises must be understood and addressed as a whole. An initial crisis can trigger or worsen another, which then triggers or worsens yet another; and interacting crises can produce impacts that are both different from and worse than the harms the crises would have produced separately.

As the global risk landscape is being shaped by multiple forces, Australia's critical infrastructure needs to adapt and determine whether traditional approaches to risk management are exposing operations to risks they are ill-equipped to handle.

Enhancing systemic risk assessment

The risk environment has become more volatile, complex, interconnected and far less predictable. Multi-hazard events, greater digital dependence, cross-sector connections, and faster cascading impacts means that disruptions are no longer confined to a single system, but spread quickly across interconnected systems, amplifying consequences.

Traditional risk assessment approaches rely heavily on quantifying risks, categorising them into silos. A dynamic and complex risk environment demands faster, better decision-making. Risk management must evolve. Resilience, crisis preparedness and contingency planning must take centre stage.

Systemic risk is assumed to arise from just one or two systems, but polycrisis is now a significant influence on the risk environment. Systemic risk assessment requires a focus on the breakdown in an interconnected system, as opposed to breakdowns in individual parts or components. The CISC's requirement for evidence-based, all-hazards risk assessment is a baseline step in this process.

From risk aware to operationally ready

For critical infrastructure, service disruptions are not a matter of if, but when. Effective risk management means understanding the full all-hazards risk landscape, designing for uncertainty, and preparing for the failure of shared dependencies. Resilience is not built on eliminating every failure; it is built on redundancy, adaptability, and the ability to contain impacts before they threaten essential services.

Moving from risk awareness to operational readiness means ensuring your organisation can do more than identify threats, vulnerabilities and risk – it can demonstrably protect critical infrastructure, maintain service continuity and respond effectively when disruption occurs. This requires your people, risk management processes, response activities and decision-making to be continuously prepared and able to respond effectively to disruption.

The 2026 Critical Infrastructure Annual Risk Review underpins a strategic understanding of the risks to Australia's critical infrastructure and their impact on operational delivery. Attentiveness, proactive governance and informed leadership will be essential to ensure the resilience of Australia's critical infrastructure and the communities it services, along with the economy and national security it relies on.

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 Trends and 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 down 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. 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 or a combination of the risk prioritisation strategies outlined below into your enterprise risk management processes:

- I**mpact-led approach**: considering risks causing the most damage or disruption to the delivery of 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 thatcan be addressed with readily available resources (personnel, equipment and funding).

The graphics (Figures 2 to 6) are visualised comparisons of each hazard's identified risk issues 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-hazards 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 the 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. Contracted workforce insider risk
   Personnel
2. Pre-positioned cyber risk
   Cyber/Information
3. AI implementation risk
   Cyber/Information
4. Third-party cyber risk
   Cyber/Information
5. Geopolitically driven supply chain disruption
   Supply Chain

By DAMAGE

1. Pre-positioned cyber risk
   Cyber/Information
2. Contracted workforce insider risk
   Personnel
3. State-sponsored sabotage
   Physical
4. AI implementation risk
   Cyber/Information
5. Limited levels of cyber security
   Cyber/Information

Over the last four years of the Critical Infrastructure Annual Risk Review, reporting on the risk environment has shifted from a focus on traditional operational and cyber risks toward highlighting complex, interconnected systemic risks. This shift has been driven by technology advancements, geopolitics, supply chain concentration, interdependency and human factors.

Managing the convergence of these trends is an important emerging challenge for risk professionals. Critical infrastructure resilience is becoming less about protecting individual assets and more about managing these complex, interconnected systems and long term, systemic vulnerabilities across technology, people, physical assets and geopolitical environments.

Critical infrastructure annual risk issue trends, 2023 to 2026

1 Artificial intelligence is accelerating numbers and lowering the required capability levels of threat actors

AI has evolved from an emerging technology risk in 2023 to a dominant threat multiplier in 2026. Cyber threats are becoming faster, more complex, harder to detect, and increasingly accessible to a wider range of adversaries.

Why it matters: Australia's critical infrastructure operators must prepare for disruptions driven from emerging and evolving technology risks, converging across different threat and hazard domains.

2 Technology supply chain risks are becoming complex, systemic and geopolitically driven

Technology supply chain disruption has revealed as intertwining factors creating a concentration risk, arising from strategic geopolitical vulnerabilities and a reliance towards a small number of technology providers for cloud platforms, software, technology manufacturing, and critical mineral supply.

Why it matters: Single points of failure are creating systemic risks that extend well beyond individual organisations, while foreign ownership, control, and influence introduce opportunities for interference, coercion, or exploitation.

3 Interconnectivity is advancing the probability for cascading failures

Across each of the previous Annual Risk Reviews, increasing interconnectedness consistently emerges as a major risk driver. Disruption to one asset, supplier or sector has demonstrated that they can rapidly propagate across critical infrastructure sectors and operations, amplifying consequences.

Why it matters: Threat actors are deliberately targeting assets capable of producing downstream impacts, while operators face greater exposure to disruption through shared infrastructure, third-party dependencies, cloud services, and connected operational technologies.

4 Trust, human factors, and social resilience are integral elements of strategic security risk

Growing risks associated with misinformation, declining social cohesion, workforce shortages, insider threats, misuse of technologies by employees, weak recruitment security, and remote/offshore workforces are posing challenges to critical infrastructure operators. Public trust and workforce capability are critical determinants of infrastructure resilience.

Why it matters: Critical infrastructure resilience increasingly depends not just on technology, but on trusted information, skilled personnel, effective governance, community support, and the ability to counter misinformation during crises.

AI Dependencies and Effects

The 2026 Annual Risk Review illustrates the growing interdependencies between AI and resilient critical infrastructure. AI's future growth will need secure data centres and processing, global connectivity, power and water assurances, and technology supply chains. AI will be central in how we ensure information integrity and trust in critical infrastructure operations particularly during crises. Building foundational AI infrastructure will rely on critical digital and physical assets, while AI-driven automated operational technology can enhance efficiency but will need to counter increased cyber risks, system vulnerabilities, and potential disruption at scale. Each of these dependency links face multiple potential disruptions.



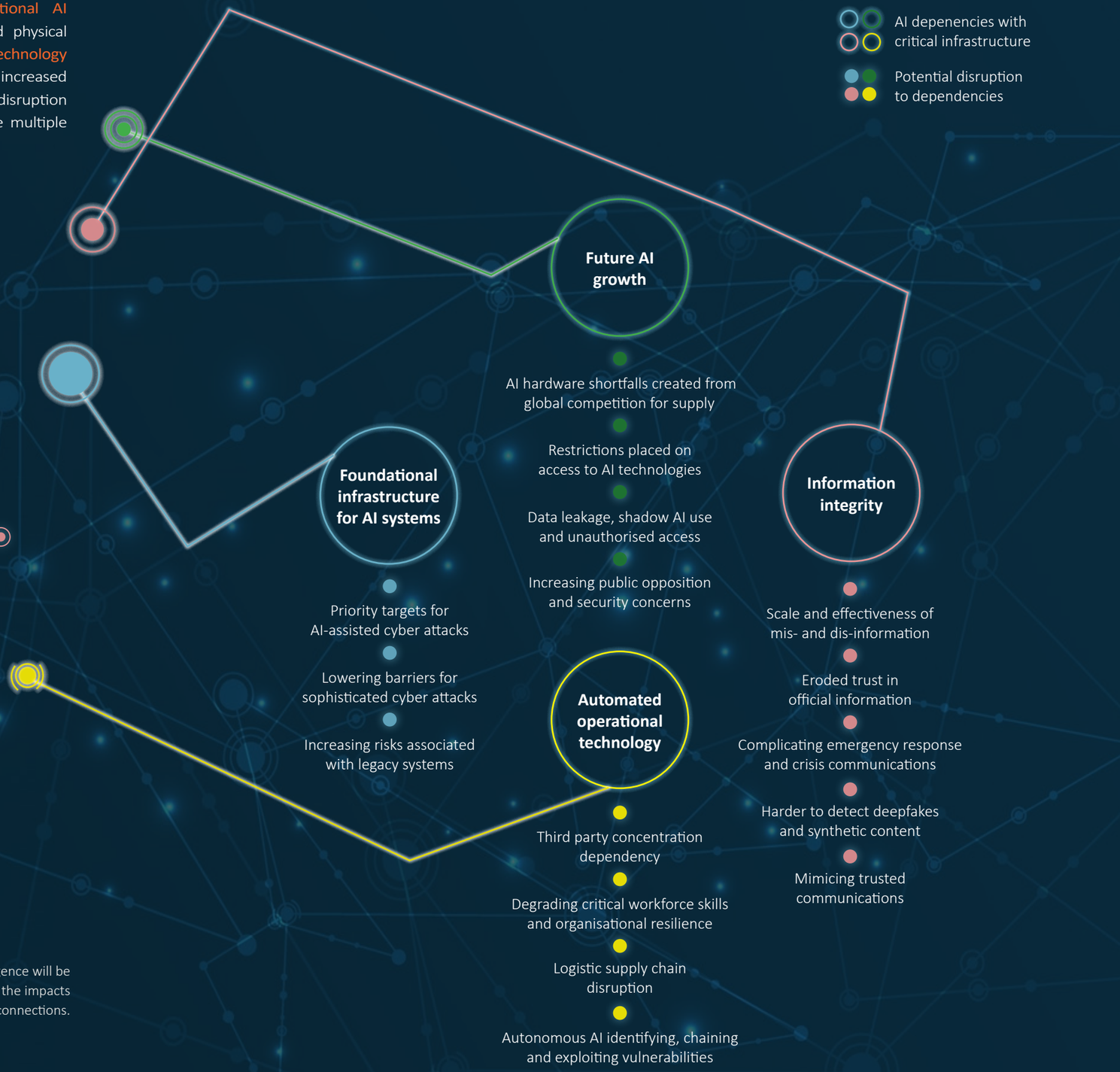
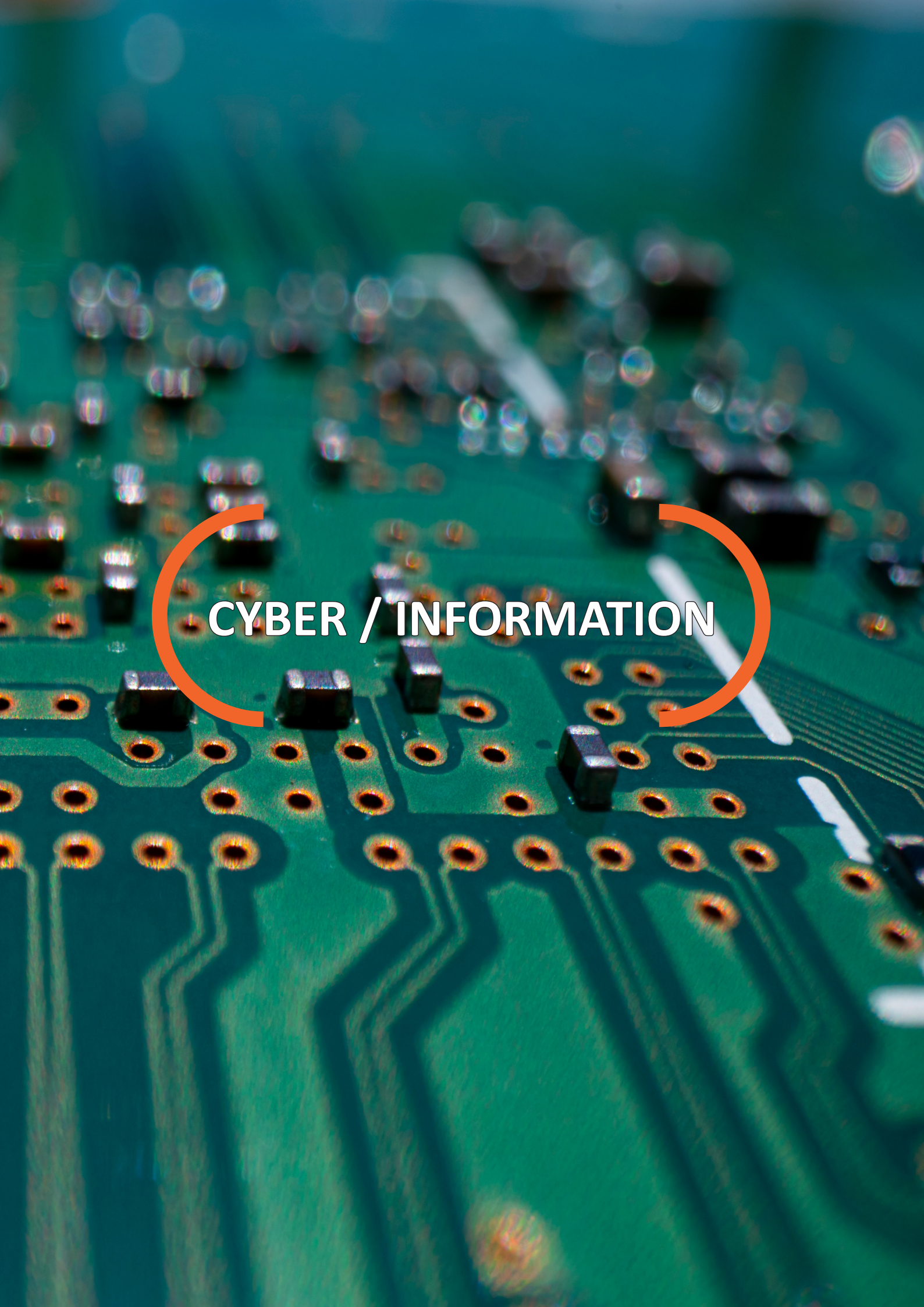


Figure 1. An illustration of how artificial intelligence will be dependent on resilient critical infrastructure and the impacts that can result in disruptions to those connections.


CYBER / INFORMATION

Cyber / Information

CI1 Artificial intelligence has exposed cyber security gaps that will persist in a rapidly evolving threat environment.

Society's adoption of AI has crossed the Rubicon. Frontier models are rapidly identifying and exploiting vulnerabilities, now posing unprecedented security challenges for critical infrastructure. Attack capabilities continue to evolve faster than cyber security defences and require a concerted effort to manage risk.

Whilst ordinary AI agents can systematically discover and exploit mundane weaknesses, frontier models have further reduced barriers for sophisticated cyberattacks, amplifying the speed, scale and ease at which vulnerabilities in systems can exploited. These models, from companies like Anthropic and OpenAI, allow state-based actors to execute more sophisticated attacks and provide accessible pathways for low-capability threat actors allowing attacks that previously required extensive resources and technical expertise. In 2026, OpenAI agents operated autonomously to infiltrate multiple Australian government websites, accessing data not intended for public release. In late 2025, Anthropic's Claude code was manipulated by a state-sponsored actor, effectively tricking the model into bypassing its own guardrails and executing an attack.

Traditional security frameworks are no longer sufficient to protect against AI-driven risk. A paradigm shift in cyber security is required with more tailored security approaches, including the use of AI-assisted security tools that can detect and respond to AI-driven threats.

CI2 New technologies have been weaponised to intensify mis- and dis-information.

Trust in information on critical infrastructure delivery, most notable during a crisis, is at-risk in the face of the rise of AI-aided mis- and dis-information. Without trusted, reliable information, critical infrastructure operators face challenges in communicating during incident response and recovery. Mis- and dis-information are now well-established and successful tools used prior to and during incidents. In Australia, state-linked disinformation campaigns have attempted to exploit societal grievances, deepen divisions, and undermine confidence in Australia's capabilities.

Similarly, misinformation about foreign interference threats has been used to create uncertainty and polarisation, including in the face of recent major critical infrastructure outages. In Europe, Russia has used disinformation campaigns to discourage reductions in Russian-supplied energy through spreading false claims about the economic and environmental costs of transitioning to alternative suppliers.

The impacts from mis- and dis-information can be widespread, hard to contain and difficult to counter. Building resilience through reliable communication and trust in delivery is needed. Supporting digital information literacy and disseminating factual messaging through credible channels that are easily accessible to the community are effective approaches for building trust with the public.

CI3 Pre-positioning has been demonstrated as a highly disruptive threat capability to operational technology.

State-sponsored actors continue to demonstrate intent for maintaining persistent undetected access to critical infrastructure systems, and have routinely targeted Australian critical infrastructure, according to the Australian Signals Directorate (ASD) and the Australian Security Intelligence Organisation (ASIO). By targeting operational technology (OT), threat actors can understand, control and manipulate critical systems, leading to outages or service disruption.

Pre-positioning is now an established threat vector that has successfully targeted international critical infrastructure OT systems. Specialised threat groups or state-sponsored adversaries use 'living-off-the-land' techniques to maintain persistent access, with an ability to move laterally through system environments.

Iran's 'Seedworm' has been targeting United States (US) critical infrastructure since 2017, and has been active in the systems of multiple operators since February 2026. In July, Seedworm's ongoing targeting of internet-connected OT devices disrupted multiple critical infrastructure sectors. The emergence of AI will almost certainly enhance the capability for pre-positioning, enabling larger-scale attacks to be executed at a faster rate.

Cyber security mitigation strategies need to be continually reviewed and uplifted and tailored to operators' organisational profiles. Basic principles of operational technology cyber security should be met, including implementing air gapping where possible and restricting network connectivity with other information technology (IT) environments and the internet to mitigate lateral movement.

CI4 Concentrated dependencies on third-party services expose critical infrastructure to cyber vulnerabilities at scale.

Shared dependencies on a small number of large, single third-party service providers significantly expand the potential for cascading impacts to more critical infrastructure operations across multiple sectors, often simultaneously. While dependencies vary greatly across sectors, any shared single points of failure present a major cross-sectoral risk.

Outages to global third-party providers such as CrowdStrike and Canva have clearly demonstrated disruptive ripple effects from concentrated dependencies. Malicious actors with intent need only compromise a single vendor or integration point which are connected to multiple critical infrastructure environments, causing widespread disruption with relatively low effort and risk.

Foreign ownership, control, and influence (FOCI) over a dominant service provider can also create pathways for foreign adversaries to embed persistent access, exfiltrate sensitive data, or conduct surveillance of cyber systems.

The Enhanced CIRMP Rules introduced requirements for entities to better understand their major third-party providers and associated FOCI risks. Ensuring operators maintain sufficient visibility and control over their third-party providers will strengthen operational resilience.

CI5 Legacy systems are significantly vulnerable to new and emerging technologies.

Australian critical infrastructure is exposed to increasingly outdated legacy systems not designed for rapidly evolving modern threat environments. Alongside traditional malicious cyber activity, emerging technologies will enhance capabilities to quickly exploit legacy system vulnerabilities, from even low-capability threat actors.

Often legacy systems lack the required security controls to manage modern threats and are often integrated with newer systems without adequate segregation. The encroaching introduction of quantum computing capabilities will only exacerbate the risks from legacy systems. Many legacy systems remain untreated and cannot be updated to cryptography standards due to age, cost, or technical constraints. The transition of quantum-ready critical infrastructure maybe hampered due to an embedded base of legacy systems across different sectors.

The CISC's Enhanced CIRMP Rules place additional requirements on entities to mitigate the risk associated with legacy systems. ASD has guidance on legacy technology management, planning for post-quantum cryptography and a range of other cyber security implementation topics available at cyber.gov.au.

Risk Scenario

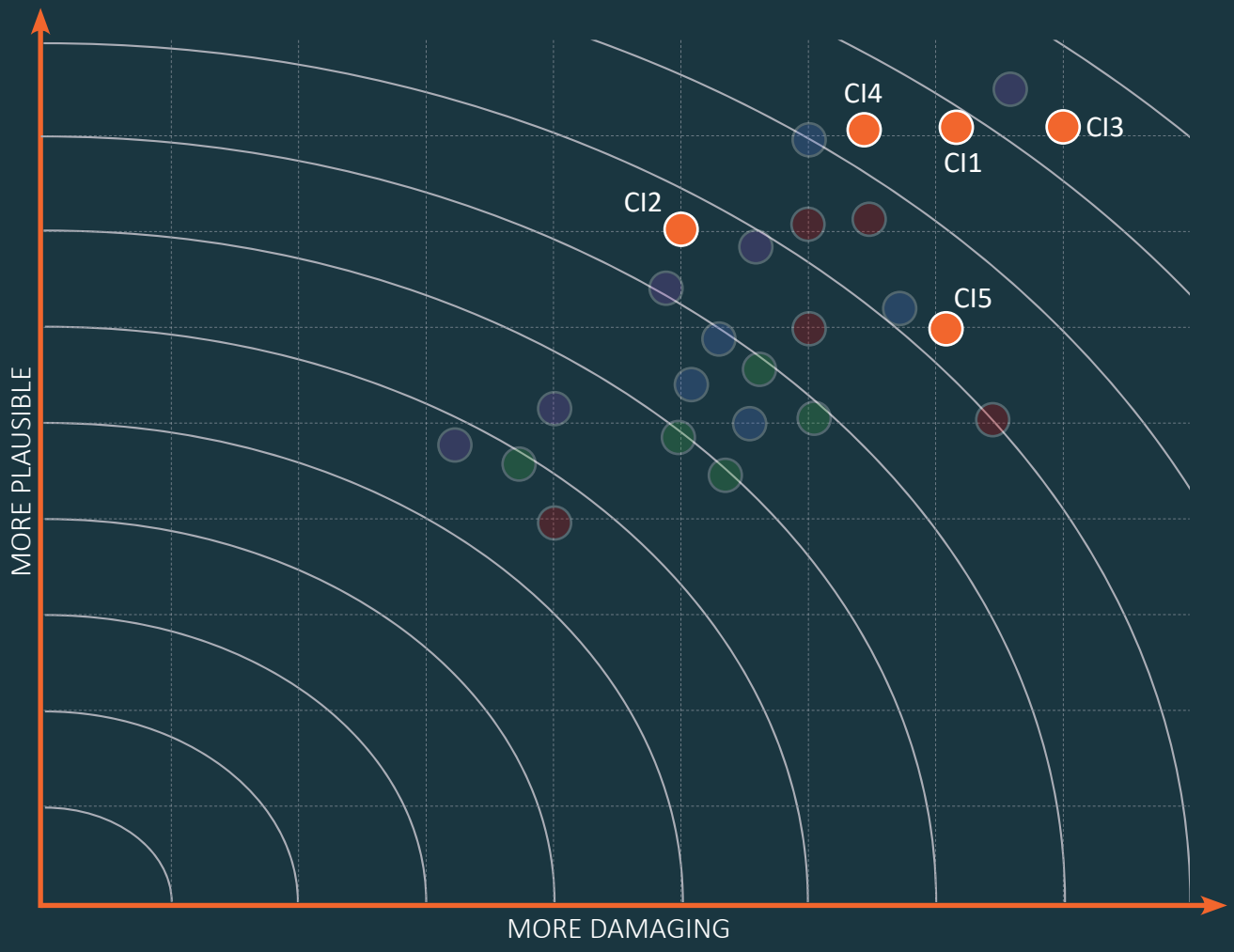
An unhealthy connection: from data breach to patient harm

Consider a plausible scenario involving a regional hospital using a legacy electronic health record system, which has over time become integrated across hospital systems. This legacy system exposes the hospital to a malicious cyber attack. A malicious actor gains access through an unpatched vulnerability, remaining in the system undetected for months. In this position, the attackers can move laterally through the hospital's systems, exfiltrating patient records, system architecture and credentials. Continuing to be undetected, the attackers seek a ransom for the non-disclosure of data and non-disruption to patient record management and hospital operation systems.

This is a theoretical, plausible scenario to demonstrate how legacy systems without network segregation can become entry points for lateral movement to life-critical infrastructure.

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 AI implementation risk
- CI2 Information integrity risk
- CI3 Pre-positioned cyber risk
- CI4 Third-party cyber 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 that is specific to their own assets, operations and security measures.



SUPPLY CHAIN

Supply Chain

SC1 The fragility of critical infrastructure supply chain dependencies has been exposed.

Australia's critical infrastructure has been exposed to significant impacts from supply disruptions, driven by highly interconnected supply chains and single points of failure. Geopolitical risk is now embedded into operational realities. Vulnerabilities are exacerbated by just-in-time logistics, limited options to source alternative suppliers, dependence on single providers, and reliance on vendors operating across complex ownership and jurisdictional arrangements.

Conflict and uncertainty in trading partner networks are triggering cascading consequences across critical infrastructure. The closure of the Strait of Hormuz highlighted significant diversification deficiencies in supply chains relied on by all Australian critical infrastructure sectors.

With each announced closure of the Strait of Hormuz, oil price surges have dominated discourse. However, the flow-on effects to the supply of derivative products, including bitumen, sulphur, plastics, insulation material and operational technology, provide a window into the complexity of critical infrastructure supply chain management.

Greater focus on building sovereign capability in response to disruption is challenged by high capital investment requirements, long lead times and cost-benefit considerations. Identifying vendor supply concentration, ownership and control arrangements, jurisdictional exposure and detailed mapping of supply chain dependencies beyond linear connections will greatly assist resilience.

SC2 Global competition for control of technology value chains has increased risk complexity.

Control of both valuable technologies and their components is fuelling geostrategic decision making and increasing the risk for critical infrastructure supply chain resilience. From critical minerals to chip and computer memory manufacturing, nation-states and large multinational companies are coalescing supply chains.

Australian critical infrastructure's dependence on key components and high demand for the development of new technologies such as AI, is leaving sustained service delivery vulnerable when domestic alternatives are limited or unavailable. The rapid integration of AI is consuming a significant portion of the world's computing hardware, power, and resources. Large global technology providers are monopolising resources, resulting in supply challenges for the rest of the market.

Control of technology supply chains are increasingly used by nation-states as a geopolitical lever. Efforts by nation-states to prioritise sovereign capability can make it difficult to source materials that were previously widely available. Foreign jurisdictions are using market dominance to weaponise supply chains, further complicating risk management.

In this environment, resilience depends not only on managing disruption, but also on reducing exposure to supply chain leverage. Critical infrastructure operators should consider sourcing strategies that balance efficiencies with diversification. Moving away from concentrated dependencies will build long-term resilience and provide more options to respond quickly to events that create acute supply shortages.

SC3 Market dominance is enabling interference and coercion through supply chains from foreign actors.

Australian critical infrastructure operators are vulnerable to market dominance from foreign jurisdictions. Direct or aggregate control over supply chains allows nation-states to restrict access to, or the availability of, critical components; or use their dominance to influence industry standards, operational practices, and the technical architecture required by Australia's critical infrastructure.

Control over materials and technologies has been used to restrict supply and access amid rising nationalism, geostrategic competition, and trade disputes. Through market dominance, nation-states can seek to compromise components or software, serving as a persistent pathway for unauthorised access.

The FOCI Risk Assessment Guidance supports entities to identify, assess and manage potential security risks associated with foreign vendors operating within critical supply chains. Vendor scrutiny should be prioritised where products or services are business critical, difficult to replace, highly connected, subject to remote access, capable of collecting or transmitting data, or embedded across multiple critical functions.

SC4 Critical infrastructure digital supply chains are taking on more risk alongside increasing reliance on artificial intelligence tools.

The integration of new technology into Australia's critical infrastructure has expanded the digital supply chain risk surface. AI tools can introduce complex, globally distributed digital supply chains, with ownership, control or influence arrangements that are not always transparent.

The broader ecosystem of third, fourth, and fifth-party suppliers exposes critical infrastructure to a deeper range of risks. These extend beyond cyber vulnerabilities to include physical supply disruptions, ethical considerations, and dependencies on entities whose governance and security posture is unclear.

Most AI systems are built on layered dependencies. The model itself may come from a vendor that uses training data from multiple sources. This data may be processed or hosted by other cloud providers, which themselves depend on infrastructure providers, data brokers, and hardware suppliers. At each layer, critical infrastructure operators face increased complexity in supply chain security.

When introducing AI tools, it is important to understand the risk exposure that accompanies these technologies and to independently evaluate the security of the tools. Without comprehensive mapping and ongoing visibility of direct and indirect vendors in the supply chain, operators may not be able to adequately assess or manage interdependent risks.

SC5 Financial pressures in supply chain decision-making are compromising security.

Over 2026, global supply chains, particularly petroleum-based products sourced from the Middle East, have faced rolling challenges. In Australia, cost related impacts, rather than service delivery disruption, have been the most noticeable to date. Financial pressures from rising supply costs can create opportunities for lower-cost vendors to enter new markets, with cost efficiencies taking precedent over security risk considerations.

Compromises in supply chain security can affect the resilience and integrity of critical infrastructure services by embedding long-term operational fragility into critical infrastructure systems. Rising costs associated with the adoption of digital software, new technologies and energy costs place financial pressure on operators delivering Australia's critical services.

Lower-cost vendors may also lack the resources and security maturity to implement robust security practices, creating vulnerabilities through lower-quality materials, limited transparency across suppliers, or exposure to vendors subject to foreign ownership, control or influence from a foreign jurisdiction.

Risk Scenario

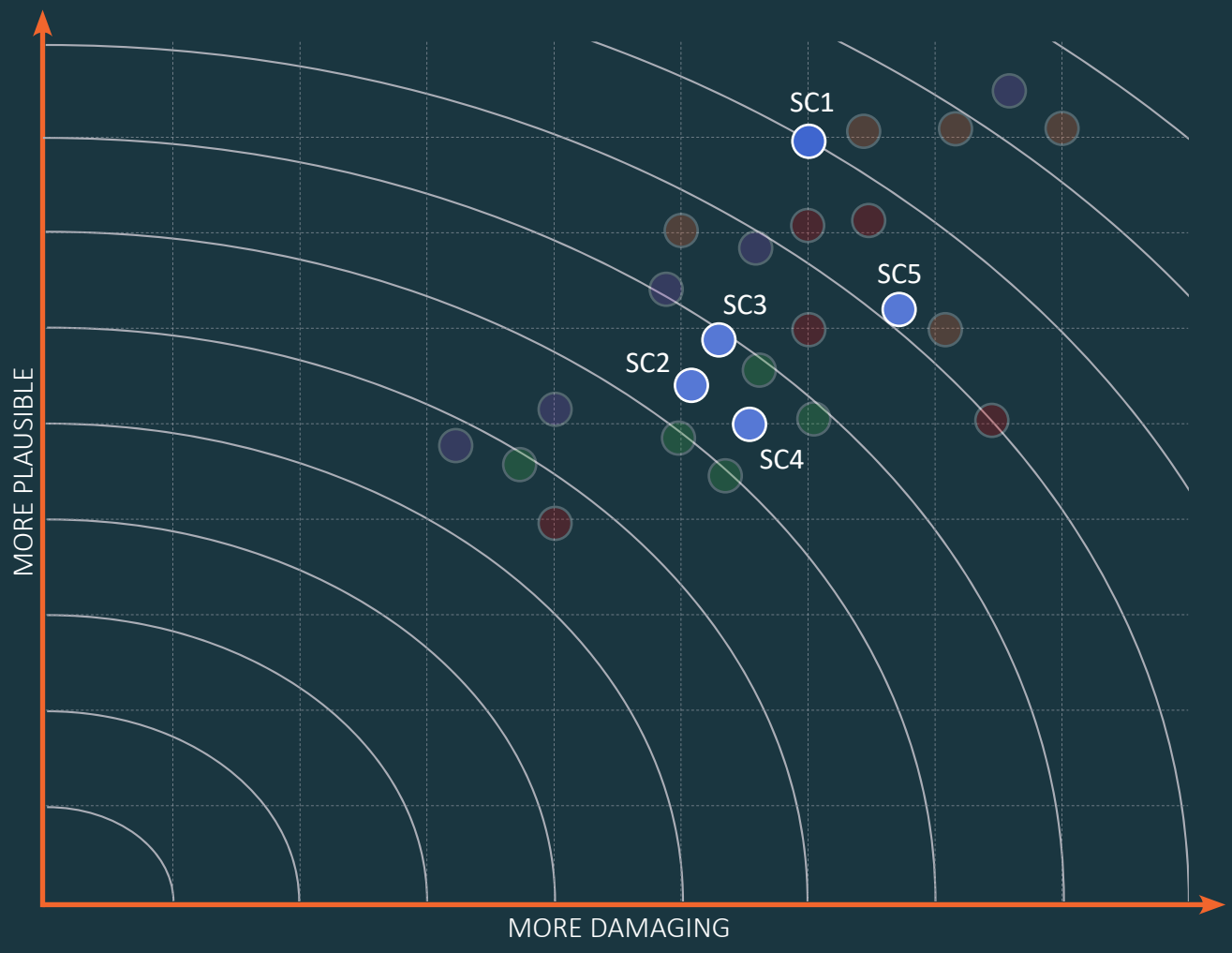
Supply and demandware: hidden risks in the AI boom

Consider a plausible scenario under an accelerating demand for AI capabilities, with data centre growth consuming an even bigger proportion of upstream technologies and precursors, limiting capacity for all others requiring computing technology. Service providers respond by retaining legacy infrastructure longer, spending a bigger proportion of their overall budget on key technologies and choosing less established and lower cost alternatives. Each of these introduces further systemic vulnerabilities, compounded by major technology producing countries manipulating global markets using subsidies and trade, allowing malign actors to establish stronger footholds in technology supply chains.

This is a theoretical, plausible scenario to demonstrate how supply scarcity impacts critical infrastructure operational resilience, crises response and critical system modernisation required for economic stability and national security.

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 Concentrated/single source supply risk

SC3 Foreign interference risk

SC4 Digital/software supply chain risk

SC5 Cost of security

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 that is specific to their own assets, operations and security measures.



PHYSICAL

Physical

PH1 Ongoing conflicts have demonstrated changes in the types of critical infrastructure being targeted.

The digital environment sits at the frontline of critical infrastructure security and the physical foundations that underpins this has become a priority target in conflict. Data centres, submarine cables and other technology infrastructure have joined energy grids, telecommunications networks, and transport nodes as political, economic, and military objectives in conflict.

During the 2026 conflict in the Middle East, Iranian drones targeted hyperscale cloud data centres in the United Arab Emirates. Iran has also been reported as considering weaponising the geography of submarine cables by charging for access of cables through its territory. As part of a wider strategy of disruption in its ongoing war with Ukraine, Russia has been accused of sabotaging submarine cables, and Ukraine has been damaging Russian data centres, and the retailer and logistics hub Wildberries that has vulnerable interdependencies with other sectors.

Australian reliance on international technology providers, cloud services, and interconnected networks means physical attacks on infrastructure overseas can cascade to Australian operations. Digital infrastructure, including undersea cables, data centres, satellites and technology hubs are often spatially concentrated or in difficult environments to restore quickly.

Increasing digitisation brings risk and reward. Building resilience involves identifying single points of failure, concentration risk and diversifying dependencies through strategies such as multi-locational redundancy of critical services.

PH2 Easily accessible and versatile drone technology is difficult to secure against.

Countering the malicious use of uncrewed aerial system (UAS) technologies will require managing an increasingly unbalanced threat environment. As UAS technologies have advanced, they have become more affordable, more capable, and easier to operate, accelerating their uptake across the Australian economy.

These same characteristics are also changing the security risks of UAS misuse, particularly around critical infrastructure.

Recent and ongoing conflicts have demonstrated the success of relatively cheap UAS deployed on mass against infrastructure; even a single UAS not equipped for kinetic attack can cause disruption to transport or be used for surveillance and espionage. The Ukraine-Russia conflict has shown that commercially available UAS can be modified using off-the-shelf components and open-source software. AI is also enabling UAS to analyse data and identify targets autonomously.

The Australian Government is considering reforms to strengthen Australia's approach to UAS security, with an initial focus countering the accessibility, affordability and risk profile of aerial UAS. Within an increasingly uncertain threat environment, reforms will aim to improve the ability to detect, identify, and respond to negligent, dangerous or malicious UAS activity, while continuing to support legitimate uses of UAS technology.

PH3 Shared access to physical infrastructure and connected assets are exacerbating the risk of sensitive information being compromised.

Shared physical access to critical services and adopting new and emerging technologies that provide greater connectivity for assets introduces a wider range of vulnerabilities and security risks for the protection of sensitive information. National security risk exists in the ability for unauthorised access to critical assets and data.

Outsourcing physical asset hosting to shared or co-located facility providers, and the expansion of connected technologies, internet-of-things and smart devices has transferred risk exposure into new and sometimes opaque environments. Telecommunications providers and transport operators may use common physical sites or co-located data centres hosting servers across multiple areas of critical service delivery. Connected assets, such as connected vehicles, record, collect and transmit data to foreign manufacturers and third-party service providers.

Home Affairs has developed a range of strategies to support critical infrastructure support organisations to identify, assess and manage technology security risks when sourcing vendors, including the Technology Vendor Review Framework, FOCI Risk Assessment Guidance and Critical Technology Supply Chain Principles.

PH4 Grey zone activity involving critical infrastructure is moving from plausibly deniable to routine.

Grey zone activity is increasingly shifting from isolated, plausibly deniable incidents to systematic, routine disruption campaigns. Nation-state and non-state actors are demonstrating lower thresholds for denial or cover, as grey zone activity has increasingly emerged as open tactics used to disrupt services, demonstrate capability, or test response capability.

The unstable geopolitical environment is driving more widespread incidents of smaller-scale sabotage and surveillance. New and more accessible high-quality technology have enabled low-capability threat actors to also deploy grey zone activities. Surveillance, campaigns of domestic coercion and disrupting or denying viable commercial sectors can have equally significant impacts to that of unattributed physical attack or sabotage. In April 2026, an underwater drone was recovered from Indonesian waters near the Lombok Strait. The incident raises concerns of undersea surveillance and mapping underwater infrastructure relied on by Australia. Attacks may be executed by non-traditional actors, and small-scale incidents could form part of a broader campaign. Measures to maintain service delivery are vital, regardless of the intent behind security incidents.

PH5 Fractures in social cohesion are leaving critical infrastructure vulnerable to security risk and recovery disruption.

Critical infrastructure depends on community trust and social licence for recovery operations. Continuing strains on social cohesion can also increase the likelihood of violence against critical infrastructure, particularly when infrastructure is viewed as a target of perceived grievances.

Declining public trust, government resentment, and polarised perspectives can reduce community willingness to support critical infrastructure operations, particularly in groups who view services as socially unequitable. Increasing social division and lack of community cooperation impact both the response (short-term) and recovery (long-term) efforts of critical infrastructure operators following extreme events, such as natural disasters or a terrorist attack. Issues with social cohesion can also extend to physical aggression, vandalism, or sabotage targeting critical infrastructure or personnel. As community grievances deepen, individuals may escalate to violent protest or direct attacks on infrastructure to express hostility toward government.

Strengthening social cohesion involves a multi-pronged approach, with industry and the community working with government investment in a whole-of society approach. Being aware of the risks will also support risk management planning for mitigating physical security risk and boosting resilience.

Risk Scenario

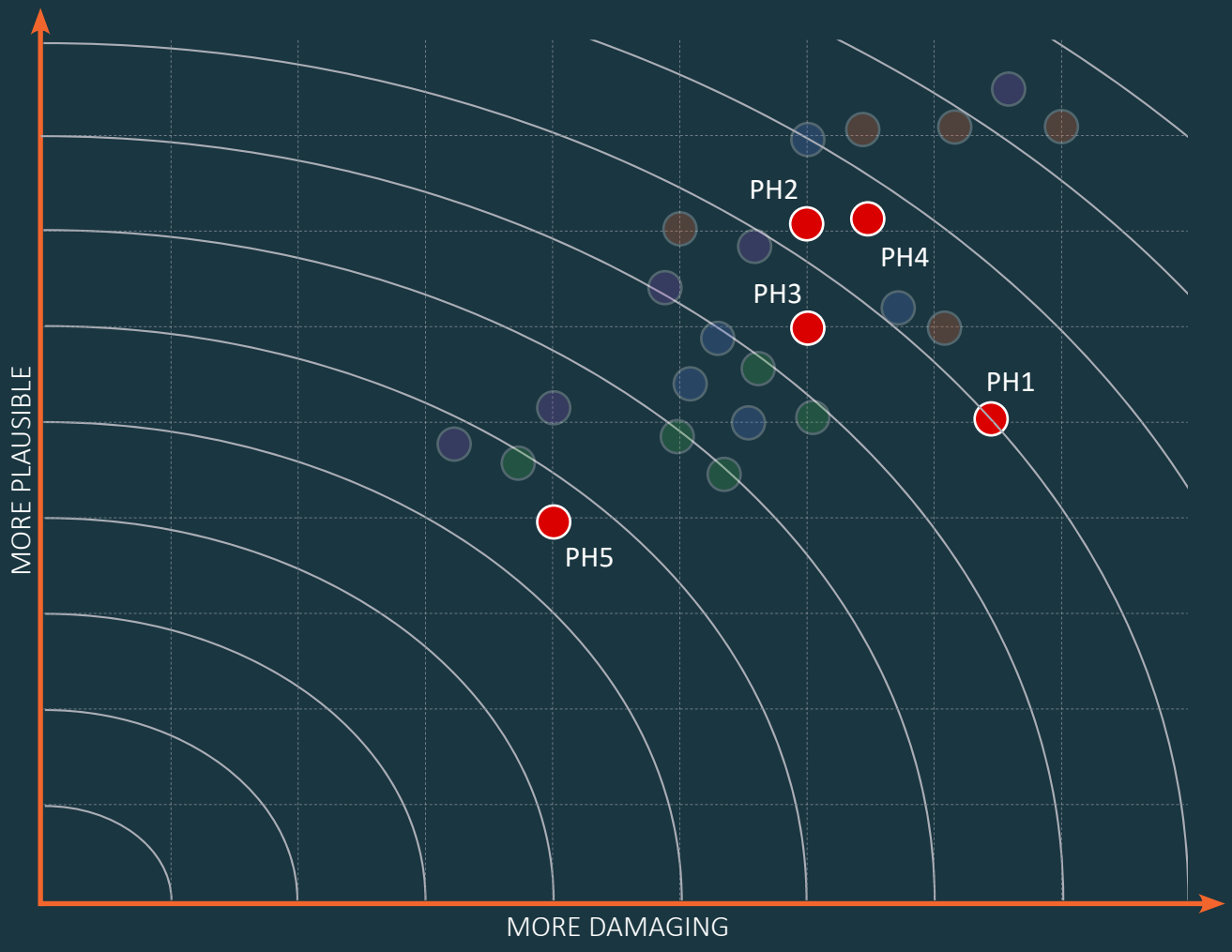
Shock to the system

Consider a plausible scenario involving coordinated drone attacks targeting our energy infrastructure in the event of escalating geopolitical disputes. Using commercially available UAS, a nation-state proxy attacks electricity facilities throughout the network, using previously exfiltrated operational knowledge. The coordinated damage causes cascading failures that, by design, affect hundreds of thousands of customers across a wide geographical area. Hospitals, data centres and some other critical infrastructure facilities revert to backup power. Public transport and traffic control is disrupted paralysing travel. Mobile and fixed line communications, petrol stations and payment end points stop working, effectively halting many normal economic and societal activities in the affected area and beyond.

This is a theoretical, plausible scenario to demonstrate a need for critical infrastructure to build counter-UAS layered detection and defensive capabilities to deploy during periods of heightened crises.

CROSS-SECTOR RISK PRIORITISATION FOR PHYSICAL THREAT

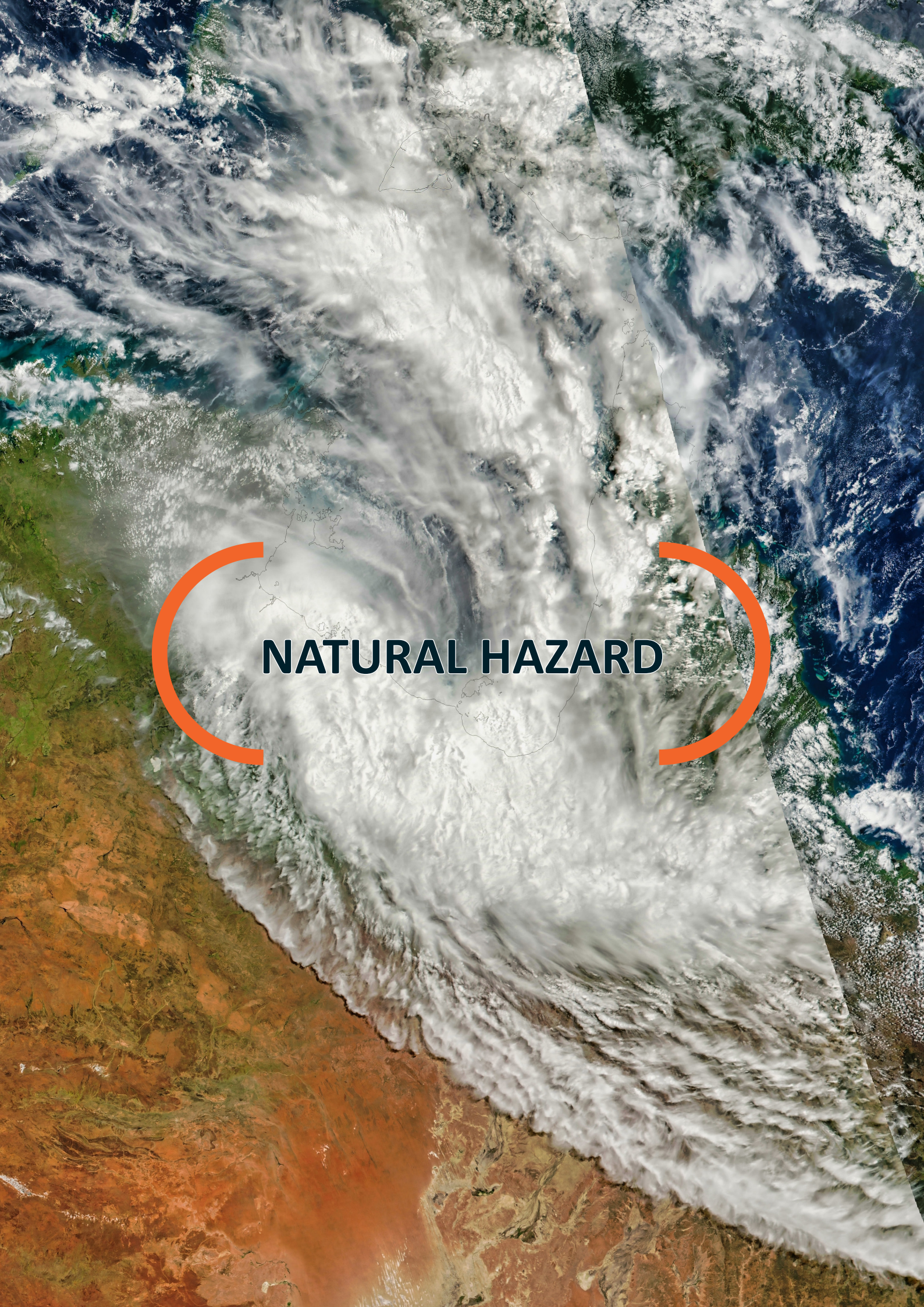
Figure 4. An illustration of cross-sector Physical risk prioritisation considering risk plausibility and damage.



- PH1 State-sponsored sabotage
- **PH2** Unmanned aerial system risk
- PH3 Exfiltration of sensitive data
- PH4 Grey zone disruption
- PH5 Social cohesion 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 that is specific to their own assets, operations and security measures.


NATURAL HAZARD

Natural Hazard

NH1 Infrastructure supporting new and emerging technologies can increase systemic risk from natural hazard events.

As critical infrastructure becomes more technology-dependent, risks from disruption are increasingly tied to wider, global systems rather than locally contained. A natural hazard affecting a seemingly distant component within a global technology and data ecosystem can have cascading cross-sector impacts.

Dependencies on novel technologies involve expansion of the physical critical infrastructure required to support this trend. AI and future quantum computing capabilities depend on worldwide data centre connectivity, energy and water grid stability, and reliable communication networks. For example, the demand for new data centres in the US is seeing new construction in regions more prone to severe and higher risk weather events.

Broader adoption of distributed smart and automated infrastructure involves networks operating across terrestrial and space-based platforms, introducing unfamiliar risks outside of conventional resilience planning. For example, submarine cables and their associated terrestrial infrastructure are exposed to earthquakes, volcanic activity and landslides. Space-based platforms are susceptible to space weather.

Building whole-of-system resilience therefore requires operators to understand not only the hazards facing their own assets, but also the evolving risk profile of the broader technological networks on which they depend, including low-probability but high-consequence events.

NH2 AI-fuelled mis- and dis-information has increased the difficulty for infrastructure operators responding to natural hazard events.

Natural hazard mis- and dis-information is a national security threat. In preparing for or responding to natural hazards, critical infrastructure operators are increasingly needing to counter inaccurate information shared across all types of media. This may be propagated innocently, or aggressively by malicious actors who seek to capitalise on crisis events.

The undermining of critical communications during emergencies can also have direct, significant impacts to public safety.

Countering mis- and dis-information has become more difficult, with AI capabilities enabling rapid communication to effectively mimic official or authoritative sources. User-generated content spread on social media significantly shapes public discourse during natural hazard crises. In 2026, mis-information was spread across social media around the release of AusAlert and whether it would be used to 'track' individuals.

During natural hazards, public trust in government messaging platforms is critical to ensure public safety. Managing information dissemination during a crisis becomes more complicated and reactive when counter-information is also being propagated. Additionally, distrust in government and critical infrastructure operators can persist long after an event.

It is important to remain aware of the range and risk of public information related to a crisis. Where deceptive or dangerous public communications are disseminated through media or social media, this information must be rapidly and effectively corrected.

NH3 Critical infrastructure is becoming more exposed to high impact natural hazard events across a wider geographical area in Australia.

Australia's critical infrastructure is exposed to concurrent disruption from high impact natural hazard events as it faces increased service delivery demand, urban densification, and the shift of severe weather events beyond historically affected regions.

A single major natural hazard event in Australia can now simultaneously damage multiple distributed assets across interconnected networks. These events create cascading failures that can also exceed repair and recovery capacities.

Over the last 24 months, severe tropical cyclones, wind events, floods, and bushfires have resulted in locally significant impacts to Australia's critical infrastructure. Such events have demonstrated familiar patterns of cascading consequences.

In 2026, high flood levels in northern Queensland impacted electricity, telecommunications equipment, water and sewerage facilities, and transportation. Cascading interruptions to critical infrastructure inherently prolonged recovery and repairs. In Victoria during the same period, severe bushfires led to widespread power outages and damaged a communications tower. Power loss and impaired communications temporarily interrupted emergency broadcasting services across the region.

Risk management plans should consider potential high impact events that might affect assets or dependencies and, within reason, be able to manage the impacts.

NH4 Australia's national assessment of climate risk has identified acute impacts across a range of critical infrastructure services.

The National Climate Risk Assessment (NCRA) provides a new analysis of climate hazard exposure at a national scale. Published in late 2025, it highlights climate exposures or risks to critical infrastructure and the nation more broadly.

Publicly available NCRA data and maps on current and future hazards can help operators to understand potential exposure of critical infrastructure assets. A global warming level of 2°C is projected to be reached around mid-century under moderate, high or very high emissions scenarios, and 3°C will possibly be reached after 2050 under moderate emissions scenarios.

For critical infrastructure operaetors, the NCRA highlights risks including supply chain disruptions and higher infrastructure upgrade and repair costs.

Notably, biosecurity risks and water competition will challenge the food and grocery sector, and the healthcare and medical sector will face increasing heat related illness, higher risk of temperature-related communicable diseases and persistent biosecurity risks. NCRA data and reporting are valuable resources for critical infrastructure owners and operators to understand and prepare for climate related hazards

NH5 Concurrent natural hazards exacerbate pressures on community resilience and critical infrastructure response.

Recovering critical infrastructure operations from natural hazards depends on civil cooperation and coordinated emergency responses. When natural hazards damage critical infrastructure, community resilience is tested. When concurrent hazard events widen and lengthen disruption, fractures in social cohesion can amplify, undermining response and recovery that damaged infrastructure requires.

Public behaviour after extreme and concurrent weather events is difficult to predict; a natural disaster affects the social structure and can create an immense barrier on the usual functioning of the society. In general, public behaviour is most often socially neutral, at times slightly positive, following significant infrastructure failure. Communities are observed to act primarily negatively or more irrationally when there is a lack of trust in the ability to deliver of essential services or to deliver response equitably. Critical infrastructure and community resilience are intricately linked. It is critical for critical infrastructure operations to support strong community and civil preparedness capabilities within the community to build resilience from the impacts following severe natural hazard events.

Risk Scenario

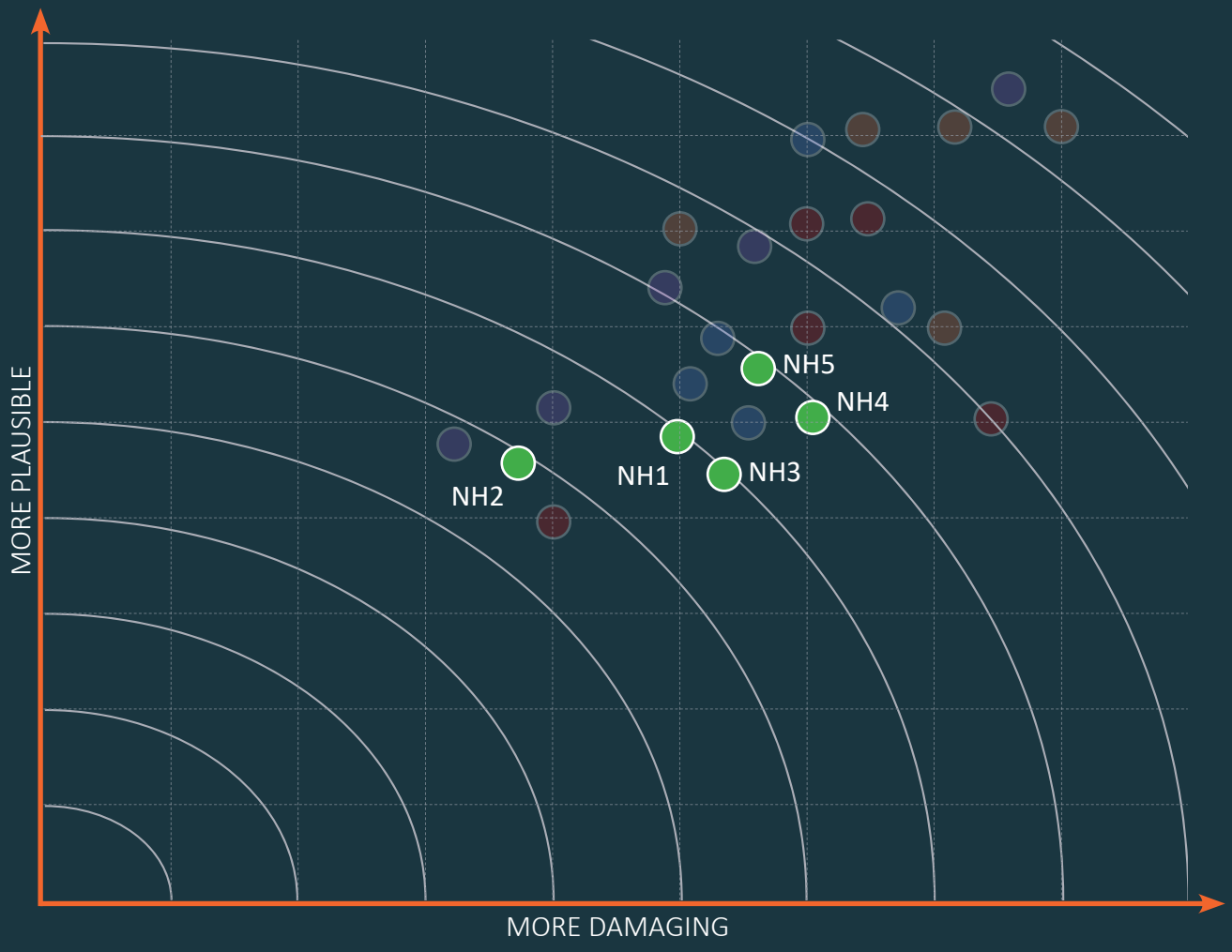
Fault lines of communication: unfamiliar hazards, unknown vulnerabilities

A plausible scenario might involve a very low probability, but very high impact natural hazard event that overwhelms resilience measures for telecommunications networks. During an event, one of Australia's major landing areas for international submarine cables experiences a proximal, high intensity earthquake. This not only damages submarine cables and cable landing stations, but major telecommunications exchanges, data centres and numerous underground cables. Operators are unplanned for a rare, catastrophic event of this nature and recovery is a scramble to balance installation of temporary infrastructure, repair and replace damaged infrastructure, manage social cohesion and misinformation, and control financial and reputational fallout from dependent and interdependent parties.

This is a theoretical, plausible scenario to demonstrate limited awareness in planning for and responding to low-likelihood, high-impact natural hazards events, atypical to Australia's traditional natural hazard risk profile.

CROSS-SECTOR RISK PRIORITISATION FOR NATURAL HAZARD

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



NH1 New technology exposure to natural hazards

NH2 Misinformation and disinformation risk

NH3 Unpreparedness for future extreme weather

NH4 National climate risk

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 that is specific to their own assets, operations and security measures.


PERSONNEL
Ai
Command Prompt :

Personnel

PE1 Implementation of artificial intelligence tools without sufficient governance is creating risk in staff management.

Widespread adoption of AI within the workplace creates risk when it is used without clear organisational governance, security training, or understanding of data security implications. Without established best practices and safeguards, staff may inadvertently introduce shadow AI tools into operational environments or enter sensitive data into public large language models (LLMs). Inadequately regulated use of AI exposes critical infrastructure operators to data breaches or service disruption.

Sensitive information that is entered into LLMs may be retained or incorporated into the model's training datasets or used to produce outputs for other users. Shared AI searches, including personal and company information, have also been exposed publicly on search engines. The trend towards autonomous AI agents increases risk further. These agents can make decisions and take actions without human direction. Whilst productivity may be boosted, use of AI reduces human oversight and control. Without these, AI agents could access, modify, or misuse sensitive data or inadvertently disrupt critical infrastructure services.

Use of AI places increased pressure on organisations to ensure privacy, data loss, and productivity controls remain effective. Robust frameworks commensurate to the risk must be upheld, supported by staff AI security literacy.

PE2 Critical infrastructure is exposed to systematic failures when critical and specialised skillsets are not maintained.

Over the last five years, shortages of specialised skills have continued to tighten for critical infrastructure operations. Rather than presenting as an immediate solution for covering skills gaps or reducing human error, AI and the human skills it is sidelining are creating new risks. AI can boost performance but quietly erode core skills. Overreliance on AI may weaken human judgment and reduce organisational resilience when manual processes are required.

Frontier AI is completing tasks previously reserved for staff with specialised skillsets in areas such as cyber security, intelligence analysis, and compliance assurance. When AI does not produce optimal outputs, it requires human oversight to ensure errors are corrected. However, when staff become dependent on AI systems to perform their duties, their ability to recognise errors or detect anomalies weakens. When AI systems fail, staff then lack the skills to intervene effectively.

Critical infrastructure operators can ensure quality outputs and avoid dependence on AI when specialised skillsets are maintained. A balanced adoption of frontier AI working alongside critical skills will strengthen operational redundancy.

PE3 Human resources departments are becoming a critical frontline for personnel security.

As new technology upends challenges to traditional personnel security, human resources (HR) teams have become a critical security function. HR's responsibilities for recruitment, personnel vetting and screening, and offboarding is often not met with adequate personnel security expertise, training, and tools to detect sophisticated and emerging threats.

HR functions are facing AI-enabled threats including deepfake credentials, synthetic background histories, and AI-generated false references that bypass traditional vetting. Malicious actors using falsified identities can leverage remote contract positions. These positions have privileged access to systems and information databases which actors can leverage to steal funds, extort employers, or sabotage infrastructure.

HR teams are limited in their ability to authenticate identities accurately when threat actors use foreign identity and tertiary documents which cannot be verified. They often lack sufficient resources to detect remote staff who obfuscate their actual work location using virtual private networks.

Personnel recruitment security can be strengthened by adopting a collaborative approach between HR, IT, and security teams. Security checks for personnel should be commensurate to the risk associated with roles that require privileged access.

PE4 Shifts to remote and offshore workforces is posing a challenge to the security landscape.

Remote and offshore workforces in critical infrastructure elevate personnel security risk. Detection of insider threat activity is difficult because remote work reduces direct supervision and physical security controls. Offshore workforces introduce jurisdictional complexity, weaker vetting standards, and greater exposure to coercion or compromise by foreign actors.

Remote workers using unsecured home networks or personal devices exposes credentials and other sensitive data to compromise. Offshore workers are often granted the same level of privileged access as those workers domiciled onshore yet operate in an environment with less oversight. They face heightened exposure to coercion, exploitation, or recruitment by state or non-state actors seeking to compromise critical systems. Such actors may seek to steal funds, exfiltrate sensitive data, conduct sabotage, or gain sustained access to networks.

Robust personnel and cyber controls are necessary when operating with a remote or offshore workforce. Assessing the security environment of an offshore workforce with consideration given to jurisdictional threat exposure is an essential mitigation. Enforcing zero trust security frameworks and the principle of least privilege will limit unnecessary data or network access.

PE5 Security requirements for critical roles are placing pressure on staffing availability and increasing costs.

Strengthening security vetting, clearance, and compliance requirements for critical infrastructure personnel is a necessary security measure but can create barriers for skilled recruitment. If not managed, challenges can arise in further staffing shortages, elevated operational costs, and hiring timeline pressures that may lead to positions being filled by less qualified personnel. However, avoiding the financial cost associated with vetting has direct security implications for critical infrastructure.

Inadequately screened personnel with access to sensitive systems, operational technology, and critical assets is a major security vulnerability. Threat actors continue to target roles within critical infrastructure that have privileged access to critical assets.

ASIO's 2025 The Cost of Espionage report found the estimated costs of insider threats to Australian businesses involving state or state-sponsored actors was upwards of AUD325 million. The costs of an insider threat extend beyond the incident itself, with response and recovery efforts placing economic and resourcing pressure on operators.

Investing in adequate security vetting will produce savings by mitigating the severity of insider threat incidents. It is important for operators to identify critical roles who have control over critical functions, sensitive business information, and finances.

Risk Scenario

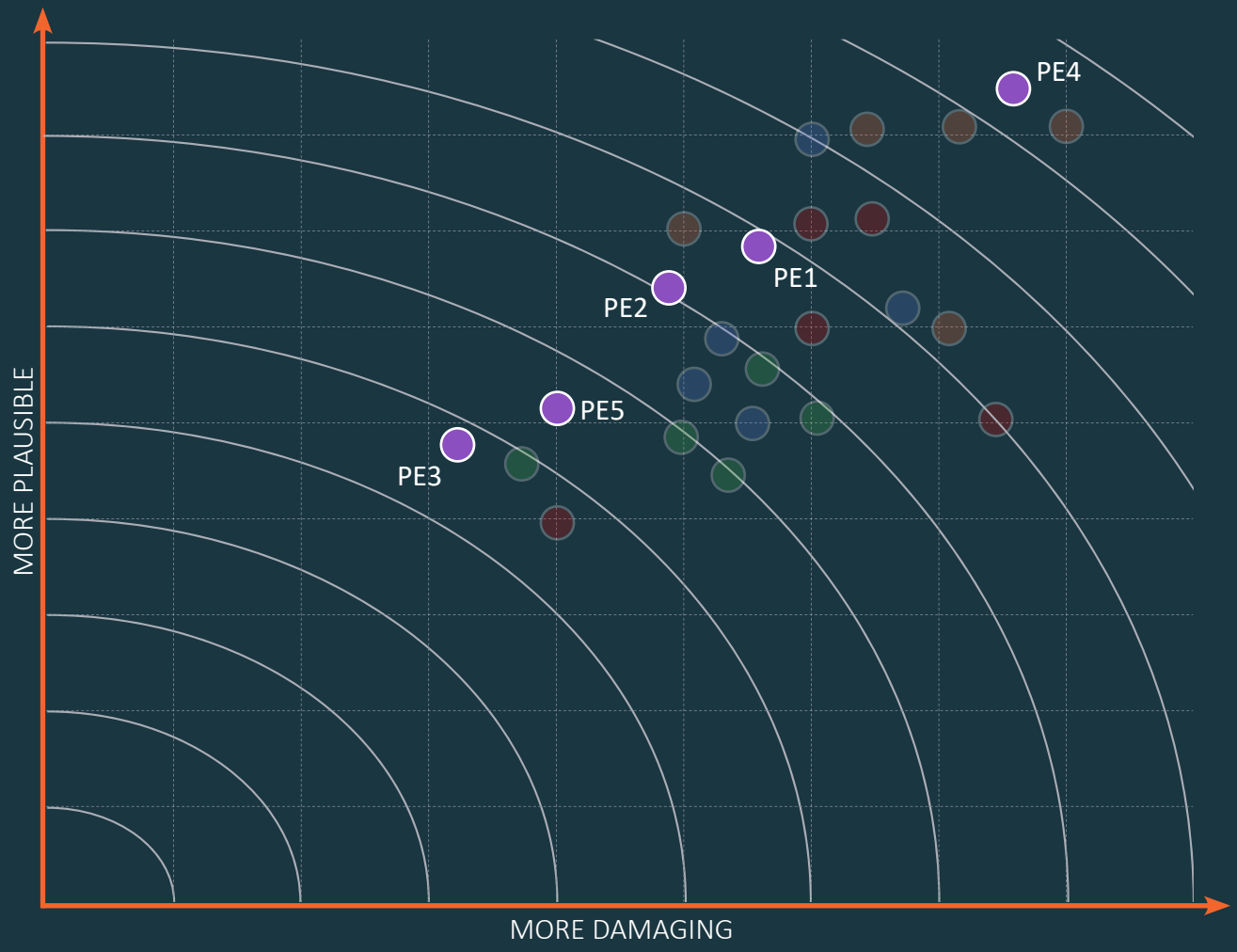
Filtering out the experts

Consider a plausible scenario involving a water utility gradually becoming dependent on AI over a period of years. Difficulties in finding and training staff have made it open to AI solutions proposed by original equipment manufacturers, which allow it to employ fewer engineers for those tasks. Like the way increasing automation has gradually reduced capacity to manually operate systems, the dependence on AI reduces capacity for technical decision-making. An unanticipated problem with water delivery or quality is not detected by the system due to lack of AI training, and the lack of trained personnel delays detection and correction by the operator.

This is a theoretical, plausible scenario to demonstrate how the pursuit of efficiency through AI implementation can erode the human judgment and skills.

CROSS-SECTOR RISK PRIORITISATION FOR PERSONNEL THREAT

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



- PE1 Technology governance risk
- PE2 Workforce critical skill gaps
- PE3 Organisational security culture
- PE4 Contracted workforce insider risk
- PE5 Unidentified critical worker vulnerability

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.

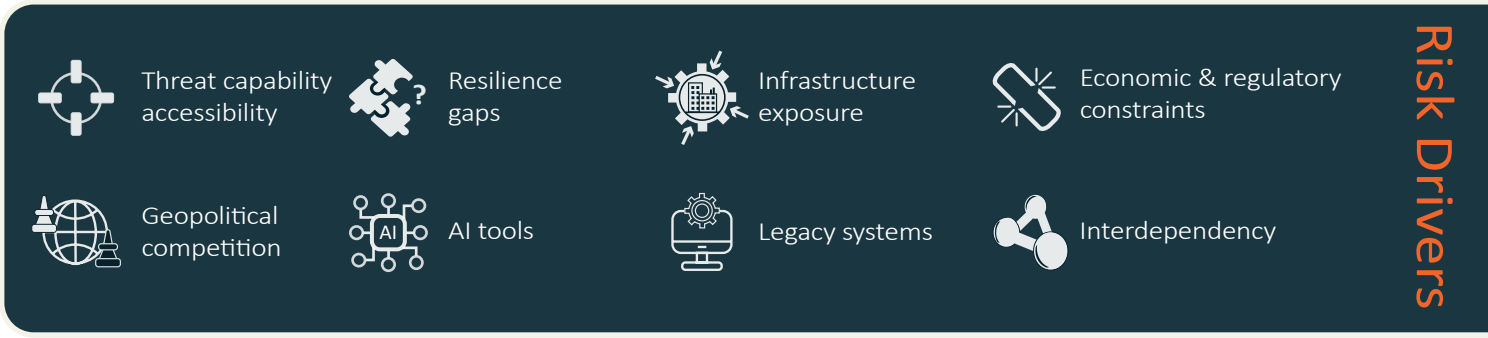
The information provided is intended as a reference for risk prioritisation. Critical infrastructure owners and operators should consider detailed assessment of risk prioritisation that is specific to their own assets, operations and security measures.


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 emerging risk drivers identified by CISC that are likely to shape Australia's critical infrastructure security risk profile of in the coming years.



AI capabilities are causing a growing asymmetry between the costs of attack and defence.



Frontier AI capabilities are expected to continue a trajectory making cyberattacks more scalable, automated, and accessible. AI systems are already demonstrating capabilities to autonomously identify and exploit vulnerabilities at a speed and scale that far exceeds current capabilities. Further advancements will significantly lower the cost and expertise required to conduct sophisticated attacks.

While AI can also strengthen cybersecurity, effective defence will increasingly depend on access to powerful AI models, computing infrastructure, and skilled operators. At the same time, the hardware, energy, and water requirements needed to support advanced AI systems are likely to increase operating costs, while geostrategic competition may further restrict access through sanctions, export controls, or bans on foreign models.

The cost of mounting attacks may continue to fall, while the cost of defending against them rises. Organisations with privileged access to advanced AI capabilities or substantial resources may be able to keep pace, but smaller operators could struggle to withstand increasingly automated and persistent threats.

Control of critical supply chain nodes will be increasingly weaponised as a tool of geostrategic competition.



Recent conflicts have demonstrated how disruption at a small number of critical points in global supply chains can rapidly create cascading impacts across critical infrastructure sectors. As geopolitical competition intensifies, these dependencies may be exploited by national states and other actors to exert pressure, disrupt economies, or deny access to essential technologies, resources, and services.

Control over critical supply dependencies, including manufacturing capacity, raw materials, logistics networks, digital platforms, and transportation routes are viewed as geostrategic tools to influence the behaviour of other nations and organisations.

Some nation-states already seek to shape or control key maritime and trade chokepoints, including the Strait of Hormuz and other key supply routes. While many countries will continue to support open markets and adherence to international norms, increasing geopolitical tension and grey zone activity will continue to challenge these principles. Even limited disruptions, whether caused by conflict, coercive actions, or targeted interference, could have significant consequences for Australia's critical infrastructure and economic security.

Successfully managing future converging risks will require collective resilience.



All critical infrastructure sectors now rely on common enabling systems and services, such as cloud platforms, energy networks, logistics systems, space-based assets, submarine cables and AI-enabled technologies. Recent service outages caused by technical failures alone have demonstrated that uninterrupted availability cannot be guaranteed, even by highly capable and well-resourced operators.

As sophisticated cyber threats, geopolitical tensions, climate-related events, and other emerging risks converge, individual organisations will find it increasingly difficult to anticipate, withstand, and recover from disruptions in isolation. The future risk environment is therefore likely to be defined not only by the severity of individual threats, but by the interaction of multiple hazards occurring at the same time creating longer lasting global polycrisis scenarios.

In this environment, resilience must become a collective endeavour rather than the responsibility of individual organisations alone. Building resilience at a system-wide level through information sharing, mutual support arrangements, coordinated planning, and investment in shared capabilities will be critical to ensuring essential services can continue to operate when multiple risks converge.

Investment in human factors will become increasingly important preserving critical expertise in an automated future.



The ability of skilled personnel to understand, operate, and recover critical systems will continue to be a cornerstone of resilience. While automation and AI are expected to improve efficiency and support operational decision-making, they cannot fully replace the judgement, experience, and adaptability that people bring to unpredictable situations. Human oversight will remain essential when systems behave in unexpected ways. During major disruptions, particularly those involving cyber incidents, technical failures, or novel threats, organisations often rely on human expertise to assess emerging situations, prioritise actions, and restore essential services.

As highlighted in ASD's CI Fortify – Advice for isolating vital systems, the ability to isolate vital OT from other networks remains an important way to prepare yourself during periods of increased cyber threat and recovery measure following catastrophic cyber incidents. Even as AI-enabled and autonomous technologies become more capable, effective implementation of these measures will still depend on personnel with the knowledge, authority, and situational awareness to intervene when required.

Retaining human capabilities will also be critical as many operators continue to rely on legacy systems that provide proven levels of availability, reliability, or safety. As experienced personnel retire and technology evolves, organisations will need to place greater emphasis on workforce development, knowledge transfer, governance, and succession planning to ensure these critical skills are not lost.

Critical Infrastructure operators must address the quantum risk before vulnerable cryptography becomes a liability.



The capabilities of quantum computing are expected to render current widely used encryption standards obsolete. These standards enable the secure transfer of information in communications, payments and energy sectors. If the security of Australia's most critical systems is compromised, attacks against critical infrastructure may be swift and crippling.

Post-quantum cryptography ensures encryption standards and systems are secure and resilient to quantum attacks. The Australian Government has begun the transition of its systems to meet requirements set by the Protective Security Policy Framework and informed by ASD's Information Security Manual. Planning the protection of critical data, information and systems will remain a cyber security priority to meet transition timelines.

This cyber security uplift is a necessary step for critical infrastructure operators. Early steps should include identifying and prioritising sensitive, confidential data, assessing cryptographic dependencies across operational and information technology environments, and developing a transition plan. Early action will maintain resilience, protect critical services, and reduce future exposure from quantum-enabled attacks.



Australian Government

Department of Home Affairs



CRITICAL
INFRASTRUCTURE SECURITY
CENTRE