Brief: Integrating Catastrophic Risk into the Critical Infrastructure Annual Risk Review

10 September 2025

*This brief provides a short overview of catastrophic risk and its implications for critical infrastructure risk management in Australia. It provides a recommendation for the Critical Infrastructure Security Centre's (**CISC**) 2025 Critical Infrastructure Annual Risk Review (**CIARR**).*

Summary

Over the next decade, catastrophic risk – the risk of events or incidents that would significantly harm Australia's security, economy or society – will increase from a range of sources. Critical infrastructure owners and operators will play an increasingly important role maintaining essential services during shocks and crises. The CIARR is a key tool for critical infrastructure owners and operators to understand the risk landscape, so it is an opportunity for the CISC to inform them of the potentially catastrophic consequences of many threats and hazards facing Australia. We recommend that the "Looking Ahead" section of the 2025 CIARR include a short description of catastrophic risk to ensure critical infrastructure owners and operators are made aware of the full spectrum of risk they need to consider when securing their assets.

About Global Shield Australia

Global Shield Australia is an independent, non-profit policy advocacy organisation dedicated to reducing global catastrophic risk. We take an all-hazards approach to global catastrophic risk management, supporting governments to enact and effectively implement policies that prevent and prepare for all forms of risk. We are the Australian office of a growing global non-profit organisation, Global Shield, which is headquartered in Washington, DC. For more information on this brief please contact australia@globalshieldpolicy.org.

National and global catastrophic risk

Catastrophic risk is the risk of events or incidents that would significantly harm Australia's security, economy or society in a manner that is beyond our existing response capability or level of resilience. The Australian Government Crisis Management Framework recognises the need to plan for extreme to catastrophic crises (Tier 4), which are crises that:

- Are highly complex, including concurrent, compounding, and/or consecutive crisis events, resulting in interlinked and cascading consequences requiring coordination across the full range of Australian Government and national equities and interests;
- Have wide-ranging harmful impacts and consequences across multiple jurisdictions and sectors of society, and extreme to catastrophic impacts on Australians; and/or
- Have overwhelmed Australia's technical, non-technical and social systems and resources, and degraded or disabled governance structures and strategic and operational decision-making functions.

Australia's critical infrastructure owners and operators must also consider global catastrophic risk. Although no such term is defined in Australian Government legislation or policy documentation, in 2022, the US Congress passed legislation, the Global Catastrophic Risk Management Act (GCRMA), which defined global catastrophic risk as the "*risk of events or incidents consequential enough to significantly harm or set back human civilization at the global scale.*" The GCRMA names several threats of particular focus, including severe global pandemics, nuclear war, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies, such as from artificial intelligence.

In 2024, the RAND Corporation conducted a comprehensive study on global catastrophic risk, as directed by the US Department of Homeland Security. It found that "*global catastrophic risk has been increasing in recent years and appears likely to increase in the coming decade*". It also recommended a number of actions the US government could take to manage and reduce the risk of a global catastrophe. The RAND report stated that "*Building and sustaining a resilient world will require continually identifying, assessing, managing, and monitoring the sorts of risks discussed in this report and other risks that might be lurking in the shadows of society's collective ignorance.*"

Catastrophic risk and critical infrastructure

National and global catastrophic risk must be recognised as part of the risk landscape facing Australia's critical infrastructure sector. The distinct nature of catastrophic events – involving concurrent, cascading failures that overwhelm traditional response plans – necessitates explicit measures to prepare for and plan responses.

There are a number of ways that a catastrophic crisis could arise and impact Australia's critical infrastructure. This includes regional conflict, the use of weapons of mass destruction, pandemics and other animal and agriculture diseases, extreme environmental events, and the failure or misuse of emerging technologies such as artificial intelligence. Each of these threat vectors has different implications for different critical infrastructure sectors. Regardless of the specific source of the catastrophic incident, critical infrastructure owners and operators should be ready to respond to the potential impacts. To illustrate this, Table 1 (below) lists the impacts that a catastrophic event or incident could have on each of Australia's critical infrastructure sectors..

Table 1. Plausible impacts of catastrophic events on critical infrastructure sectors

Sector	Example catastrophic threat or hazard	Plausible catastrophic impact
Communications	A severe space weather incident disrupts satellite access; multiple submarine cable breaks (deliberate or accidental) degrade internet capacity.	• Nationwide loss of internet and phone connectivity, leading to economic disruption and potential for public panic. • Emergency alert systems are disrupted, responses delayed and casualties increased.
Financial services and markets	Pre-positioned malware corrupts core banking records and functions, forcing a prolonged suspension of payments and settlements.	• Payment systems fail; commerce stops and critical supply chains grind to a halt. • Financial and banking systems collapse, leading to social unrest and economic paralysis.
Data storage and processing	An AI-enhanced cyberattack exploits zero-day vulnerabilities in cloud data centers, wiping multiple Australian regions and backups.	• Critical databases attacked, corrupted or wiped could lead to public services collapse, and major disruption in health, welfare, and security systems.
Defence industry	A major power conflict erupts in the Indo-Pacific, with Australia directly or indirectly targeted.	• Large-scale war overwhelms domestic industry and logistics. • Production and supply of defence equipment severely hampered; erosion of defence capability during severe crisis.
Energy	Concurrent bushfires sever interconnectors between several States, or an extreme geomagnetic storm destroys high-voltage transformers.	• Extended blackouts lead to disruption and collapse of essential functions. • Hospitals, businesses and homes incapacitated. • Transport and logistics immobilised, leading to a stalled economy.
Food and grocery	An uncontrolled, fast-spreading agricultural pandemic combined with trade tensions leading to disruptions to critical inputs such as fertilisers.	• Production collapse, leading to mass hunger, civil unrest and rising mortality. • Supermarkets empty, leading to public panic, rationing and hoarding.
Healthcare and medical	A novel, engineered pandemic, caused by a highly transmissible, high-mortality pathogen is released, intentionally or accidentally.	• Health systems overwhelmed, leading to a collapse of hospital capacity and mass casualties. • Critical workforce shortages across all sectors due to illness and death.
Space technology	Low earth orbit collisions, possibly caused by anti-satellite weapons, create a Kessler Syndrome situation, rendering satellites inaccessible or inoperable.	• Loss of GPS cripples transport and defence operations. • No weather forecasting, undermining disaster response and food security.

Sector	Example catastrophic threat or hazard	Plausible catastrophic impact
Transport	A protracted global conflict severs access to global supply chains, including refined fuel imports.	• Essential imports cut off. • Remote and regional populations face extreme hardship.
Water and sewerage	Prolonged, nationwide energy grid collapse disabling pumping and treatment stations.	• Drinking water is made unsafe, leading to a public health crisis and mass illness. • Pumping and treatment ceases, potentially leading to widespread disease outbreaks. • Forced rationing leads to social unrest.

Catastrophic risk in the CIARR

Without greater inclusion of the catastrophic potential of these threats and hazards, the CIARR misses plausible worst-case scenarios that critical infrastructure owners and operators should be alert to. Over the next decade, critical infrastructure providers will play an increasingly important role maintaining essential service critical for Australia's security, economy and communities – given the ever-increasing reliance on these services, greater national and global interconnection between sectors, and integration of emerging technologies.

We recommend that the "Looking Ahead" section of the CIARR include a short description of catastrophic risk. The following text is a representative example of what could be included:

> *"Catastrophic risk is increasing in likelihood and complexity. Catastrophic risk is the potential of plausible worst-case scenarios — such as pandemics, major power conflict and climate system collapse — that could cause widespread, long-term harm to societies and economies. The risk of such events is growing due to geopolitical competition, progress and diffusion of critical technologies like artificial intelligence, and climate and environmental disruptions. For critical infrastructure providers, catastrophic risk matters because it could quickly and simultaneously disable multiple systems, overwhelm contingency plans, and create cascading failures across sectors. Critical infrastructure owners and operators should consider including catastrophic risk into their Critical Infrastructure Risk Management Program (CIRMP). They should also consider integrating catastrophic scenarios into resilience planning, such as by stress-testing continuity strategies against extreme, prolonged and cross-sector disruptions."*

We would also encourage the CISC to identify and include at least one example of a cascading or catastrophic hazard or threat in each of the CIARR's plausibility/damage matrices. Realistic examples provided to the private sector owners and operators would demonstrate how a hazard or threat could credibly produce consequences that would exceed their capacity to manage.

Each sector would then be able to develop a better picture of the plausible worst-case scenarios for which they need to prepare. It would also help CISC identify ways for the government to support capabilities of critical infrastructure sectors. This will aid the CIARR's use by senior policymakers and government agencies in a risk-informed decisionmaking process to improve Australia's overall resilience.