Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Annual Risk Review

First Edition
November 2023

Contact us

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

Industry Partnerships Branch,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

About the Cyber and Infrastructure Security Centre

Within the Department of Home Affairs, the Cyber and Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure regime in partnership with governments, industry and the broader community. We actively assist Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory requirements for the shared benefit of all Australians.

Our mission

Our mission is to collaboratively ensure the security, continuity and resilience of Australia's critical infrastructure. We empower Australian owners and operators to meet best-practice standards and improve the resilience of our critical infrastructure through:

- Engagement.
- Partnerships.
- Advice.
- Exercises.
- Modelling.
- Regulation

Our role as a regulator

We are committed to being a best-practice regulator. We use our integrated capabilities to improve the critical infrastructure regulatory framework.

What we do

To understand the operating environment and facilitate best-practice advice and engagement across critical infrastructure sectors, we work with:

- Governments.
- Industry.
- Current and future asset owners and operators.
- Regulators.
- Technical Advisers.
- Academia.

We bring together, and build on:

- Critical Infrastructure.
- Cyber Security.
- Aviation Security.
- Maritime security.
- Personnel Security.

We leverage partnerships across sectors and between regulators and agencies to empower critical infrastructure owners and operators to remain resilient in an ever-changing risk and operating environment.

Industry's knowledge of the different sectors, businesses, operations and processes is critical for our collective understanding of the environment and our approach to capability uplift. Our Trusted Information Sharing Network (TISN) is an example of how we enable this vital work.

There are significant benefits to be gained from proactive compliance and risk mitigation. We facilitate engagement to support asset owners and operators to meet their obligations and prepare for incidents.

Collectively, our efforts support the resilience of critical assets and the reliable delivery of essential services that underpin the enduring confidence needed for all businesses to plan, grow and thrive.

For further enquiries please contact us at:
enquiries@cisc.gov.au

Introduction

The first edition of CISC's Critical Infrastructure Annual Risk Review provides a summary of the key risk-driven issues that have been affecting the security of Australia's critical infrastructure over the last 12 months.

The review presents risk issues under each of the threat and hazard categories outlined in the Security of Critical Infrastructure Act 2018 (SOCI Act 2018) and accompanying rules for the Critical Infrastructure Risk Management Program (CIRMP).

As the Commonwealth regulator for critical infrastructure security, it is important for us to support critical infrastructure providers adapt their existing risk practices; and help organisations understand risks within the broader national security context.

Risk in the context of national critical infrastructure is related to our national and societal resilience. Disruptions to critical infrastructure can have serious implications for business, governments and the community, affecting the security of resources, supply and service continuity, and damaging our economic growth.

Critical infrastructure providers face a wide range of disruptors to the continuity of operations. Risks with the greatest impact on Australia's social or economic stability, and on its defence or national security, also need to be considered and framed within the existing risk management strategies of critical infrastructure entities.

Australia is likely to see an increase in the frequency and severity of natural hazards, and a future punctuated by more complex, cascading or compounding disasters. As Australia enters another El Niño weather cycle, in 2023 we witnessed record heatwaves and catastrophic natural hazard events in the Northern Hemisphere. Severe weather events are becoming more frequent and with longer recovery times, putting pressure on the delivery and resilience of critical infrastructure systems.

Foreign involvement is permeating into all areas of the delivery of critical infrastructure. Australia's critical infrastructure is a complex network of facilities, personnel, outsourcing, offshoring and supply chain dependencies. Foreign involvement is across all nodes of this network and has the potential to create risks to national security if the nature of this interaction is not properly managed.

Australia's critical infrastructure sectors are a deeply interconnected system of systems; significant disruption in one sector will affect other sectors. The increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities which, if targeted, could result in significant consequences for our economy, security and sovereignty.

Increasing digitalisation and implementation of new technologies are adding new entry points for cyber incidents. Over the last 12 months there Australia has witnessed the reporting of cyber incident against high profile targets, including Australian critical infrastructure providers. Rapid advancement and implementation of new technologies can severely hamper efforts to create a uniform cyber defence, in line with lower levels of cyber literacy.

Risk levels are very likely to increase during periods of heightened geopolitical tensions. Critical infrastructure remains an enduring target of interest for threat actors seeking to cause harm. Across different geopolitical conflicts, pre-positioning and grey zone cyber operations are used alongside conventional military activities for extensive targeting of critical infrastructure networks.

Supply chain resiliency is a multi-faceted strategy of proactive defence and efficient response to disruption. Australia remains vulnerable to international supply chain disruption and single source supply for critical components and services. Critical infrastructure providers need to develop adaptive supply chain resilience plans, driven by risk analysis, to withstand disruption to global supply chain networks.

Critical Infrastructure Risk and Regulation

Critical infrastructure providers are uniquely positioned to assess risk through the analysis of identified threats and hazards against their own assessment of vulnerabilities. Understanding the potential relevant impact is also important to prioritising risk and determining how best to minimise the likelihood of the risk occurring and mitigate its potential impact (Fig. 1).

Under SOCI Act 2018 and its accompanying CIRMP responsible entities are required to establish, maintain, and comply with a written risk management program that identifies and take steps, where practicable, to minimise or eliminate material risks that could have a relevant impact on their critical infrastructure assets.

The CIRMP is intended to uplift core security practices that relate to the management of certain critical infrastructure assets. It aims to ensure that responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks. More information on the CIRMP is available at **cisc.gov.au**.

Material risk is defined in the CIRMP, and includes:

a. *stoppage or major slowdown of the CI asset's function for an unmanageable period;*

b. *substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset;*

c. *an interference with the CI asset's operational technology or information communication technology essential to the functioning of the asset;*

d. *the storage, transmission or processing of sensitive operational information outside Australia, which includes:*

   i. *layout diagrams;*

   ii. *schematics;*

   iii. *geospatial information;*

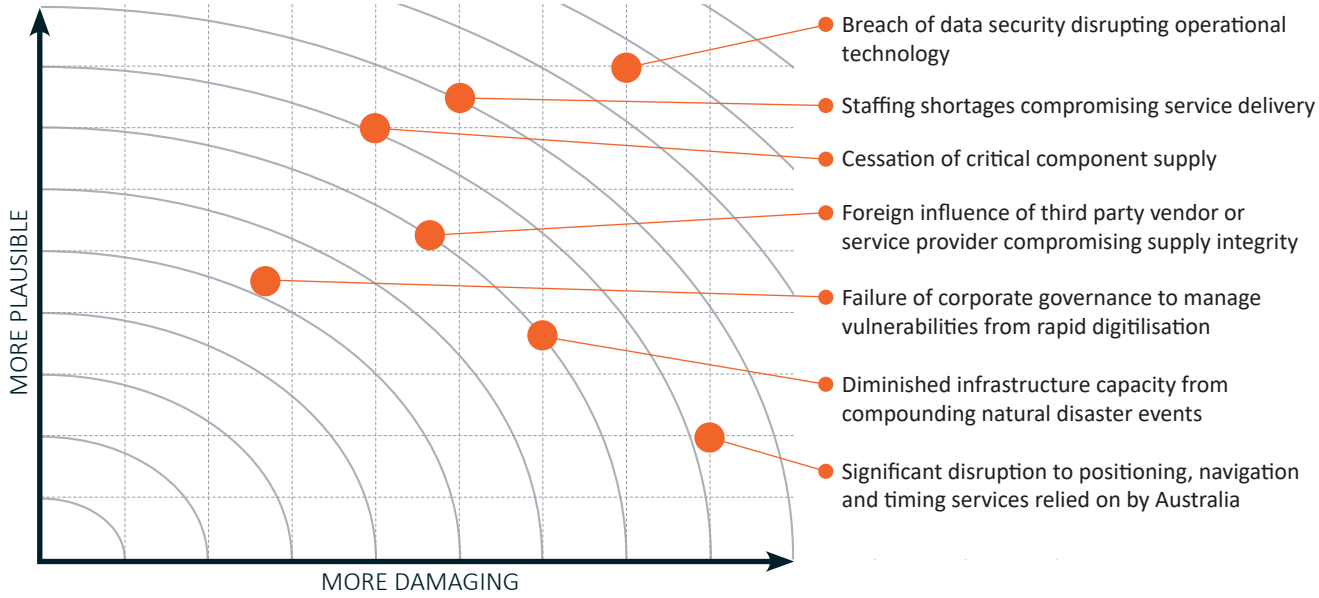
   iv. *configuration information;*

   v. *operational constraints or tolerances information;*

   vi. *data that a reasonable person would consider to be confidential or sensitive about the asset;*

e. *remote access to operational control or operational monitoring systems of the CI asset.*

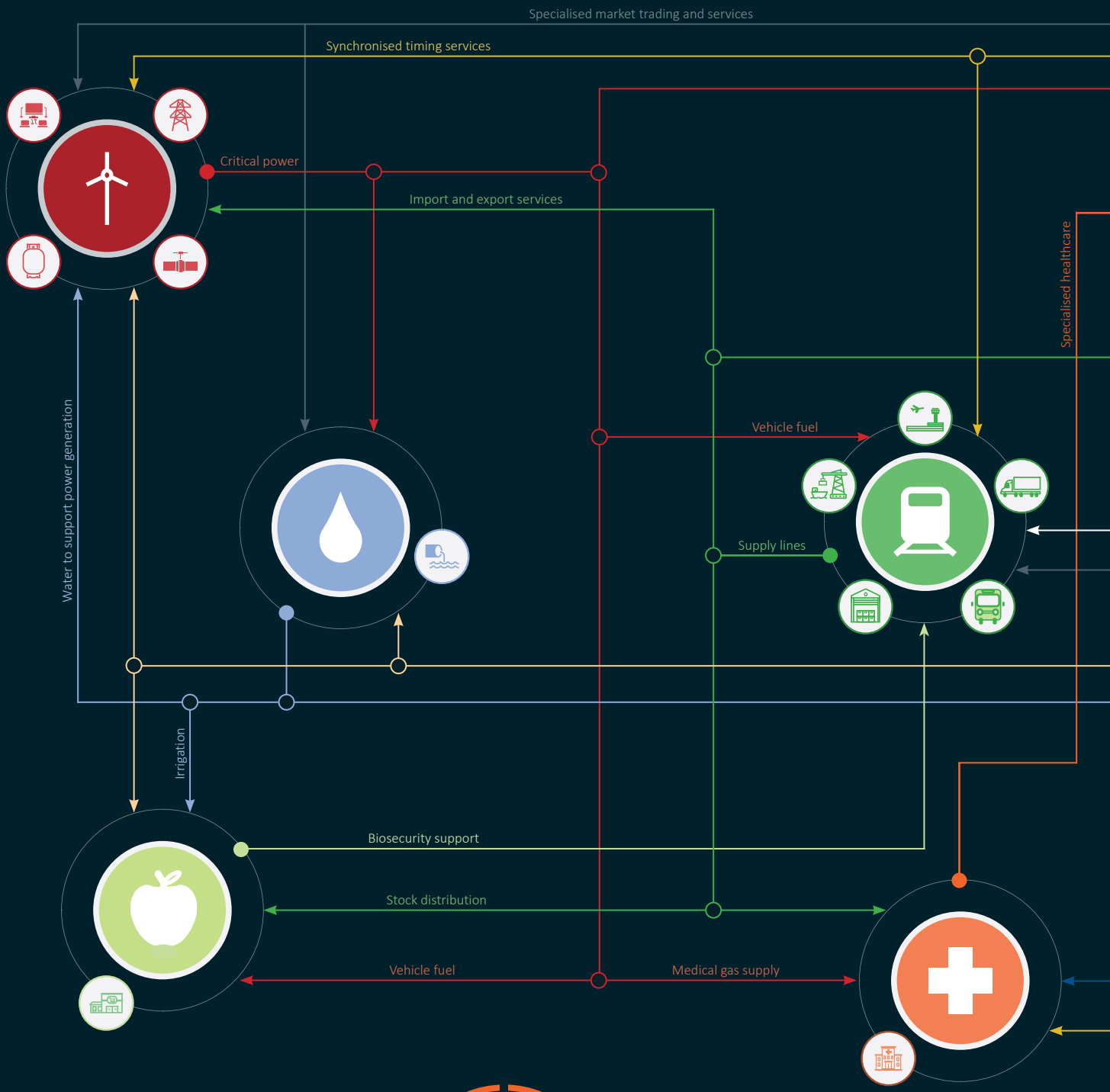
Fig. 1. An illustration of cross-sector risk prioritisation considering risk plausibility and impact.



Sector Interdependency

Modern critical infrastructure systems are rarely, if at all, self-sustained. Impacts experienced in one sector would likely be magnified across sectors through a 'creeping dependency', a growth of interdependent critical infrastructure systems (Fig. 2). It is just as likely for critical infrastructure providers to experience a disruption to critical services as a result of upstream dependencies, as they are to being directly impacted by the event.

While it is difficult to predict the behaviour of an entire system simply based on the behaviour of one of the components, relationship analysis can help understand possible impacts from cause and effect.



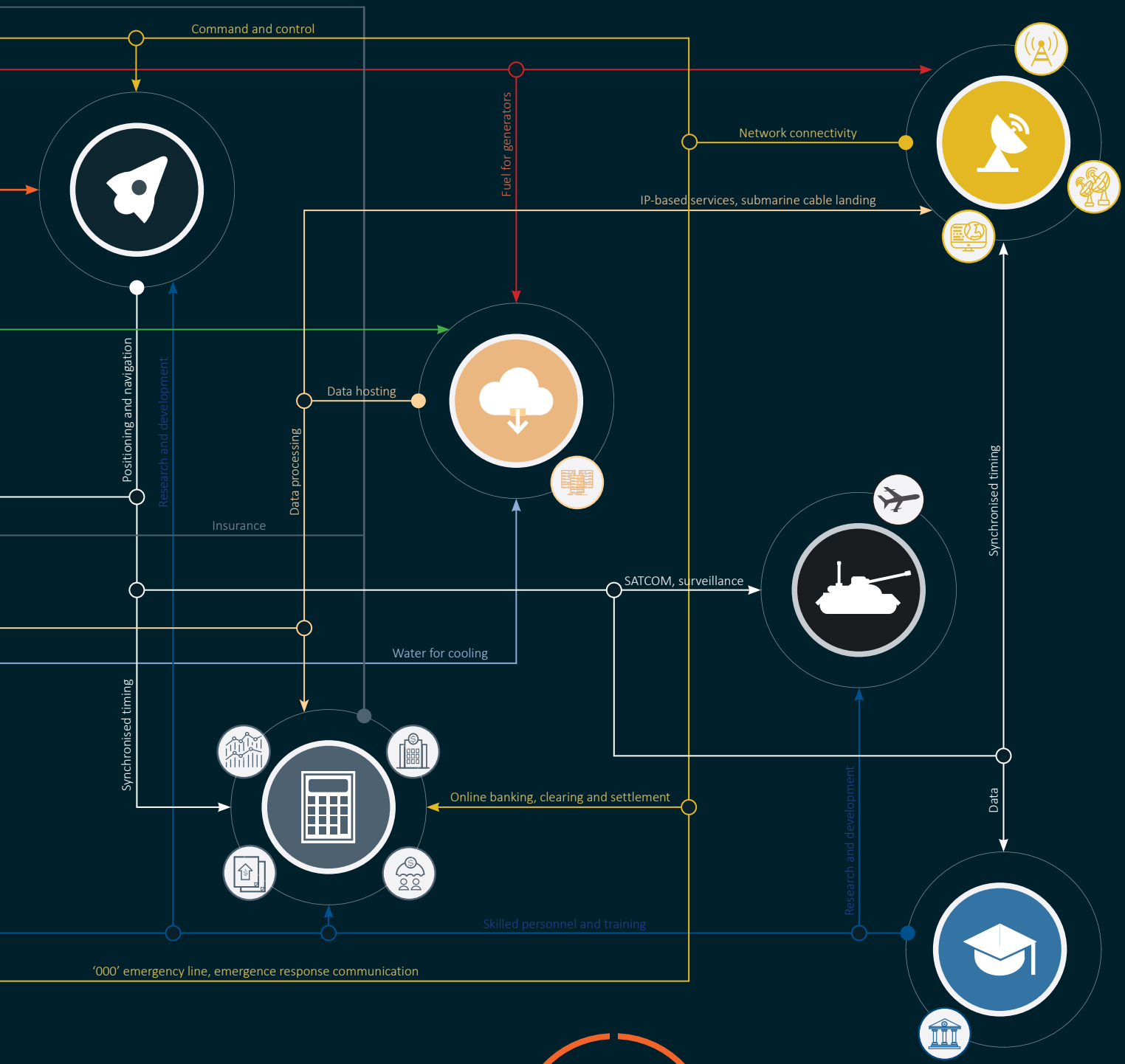
Risk assessments should consider effects that go beyond a simple linear impact causal chain, such as:

earthquake → dam failure → flood

A cascading effect can be nonlinear, where causal loop diagrams can be used to analyse linkages and 'cause and effect' relationships. Cascading effects can increase the impact well beyond the original temporal and spatial components.

A compounding effect is one where an event triggers follow-on sequences of other events that occur as a direct or indirect result of the initial triggering event, at times prolonging any initial impact.

Fig. 2. An illustrated example of key interdependency between critical infrastructure sectors.




CYBER / INFORMATION

Cyber / Information

Critical infrastructure is a high-interest target for malicious cyber activity. Australia's private and public institutions remain vulnerable to malicious cyber activity including from financially motivated and state-sponsored actors. Over the last 12 months a number of high profile incidents involving information theft demonstrated the breadth of our susceptibility to cyber threats.

Australia's critical infrastructure presents further layers of target attractiveness beyond the theft of personal identification information. A broad range of critical infrastructure can be tangibly disrupted, manipulated or destroyed as a result of malicious cyber activity. Cyber actors will also look for weaknesses in our systems to obtain valuable sovereign research and gain insights into our social, economic or technological vulnerabilities.

Levels of risk will shift with fluctuating threat environments, where critical infrastructure can become a legitimate conflict target, impacting the proper functioning of a sector and eroding public trust in institutions. In the Russia-Ukraine conflict, cyber operations have been used alongside conventional military activities for extensive cyber targeting of government and critical infrastructure networks.

In the hours before Russian military operations started in Ukraine, US satellite company Viasat, which provided satellite communication capability to Ukraine was the target of a cyber sabotage event. Targeting ground infrastructure, Russian-linked entities deployed 'wiper' malware against Viasat modems and routers, quickly erasing all the data on the system, which disrupted Ukraine's communication capabilities.

More sophistication in targeting is exposing narrow risk mitigation efforts. Cyber actors continue to scan for and exploit vulnerabilities across interconnected critical infrastructure networks. Third-party and managed service providers; physical and digital supply chains; and physical infrastructure are equally important to the operation of critical infrastructure providers.

There is vulnerability in the convergence of operational technology (OT) and Information technology (IT), and the rollout of Internet of Things (IoT) devices. Increasing sophistication of cyber incidents, such as the lateral movement of a cyber incident between systems can create catastrophic cascading consequences.

The 2021 Colonial Pipeline cyber incident in the US, which started as a ransomware attack on a corporate system, led to a decision to shut down operational systems to mitigate risk of cross-system compromise. This resulted in cascading supply chain impacts, most notably to the distribution of gasoline and jet fuel to the Eastern United States.

OT and connected systems, including corporate networks, will likely be of enduring interest to malicious cyber actors. OT can be targeted to access a corporate network and vice versa, potentially allowing malicious cyber actors to move laterally through systems to reach their target. Even when OT is not directly targeted, attacks on connected corporate networks can disrupt the operation of critical infrastructure providers.

Adoption of IoT in critical infrastructure also leads to a growing integration of third-party inputs for information, data sharing and data analytics.

Digitalisation is outpacing our cyber literacy and security practices. Rapid advancements in technology severely hamper efforts to implement uniform protection measures to reduce the risk from cyber incidents. Critical infrastructure providers have different thresholds and practices for ensuring cyber security, which introduces a range of vulnerabilities. Good cyber security practices and

secure-by-design principles can help organisations better protect their systems from cyber intrusion or improve recovery times after an event.

Significant cyber incidents can also occur as a result of human error. Poorly managed corporate systems, particularly those with remote access, can provide an attractive target for extortion, disruption or espionage.

Malicious cyber actors will target the weakest links to access multiple data-rich systems. Australia's critical infrastructure systems are highly interconnected, boosting their social and economic benefits and maximising critical service delivery. This interconnection also increases risk. Every interconnected device, technology or system is a potential avenue to access our critical infrastructure entities.

Pre-positioning for malicious activity in Australia's critical infrastructure is a known, but hidden risk. The pre-positioning of malicious code in critical infrastructure networks as a preparation for future attack is an ever present challenge for critical infrastructure providers. The capabilities underlying this threat continue to advance and potential impacts from pre-positioned malicious code retains a level of unpredictability or both the intended victim and threat actor, further complicating mitigation efforts as the full extent of this threat remains elusive.

In July, the US identified a possible malicious code hidden inside critical infrastructure networks providing power, communication and water supply for some military sites, and surrounding civilian populations. Removing any identified code may alert adversaries to what has been found, aiding future attempts.

Interconnected critical infrastructure networks and third-party providers across supply chains expands attack surfaces for supply disruption. This includes remote access and management solutions, which are increasingly present in critical infrastructure networks.

Any cyber incident targeting our critical infrastructure could have major consequences. A sustained disruption in one area of the ecosystem may cascade through other sectors, potentially leading to widespread disruptions to the operations and service delivery of key sectors.

Next generation technologies will change the way we need to assess risk. As our critical infrastructure sectors are willing to adapt new technologies into operations and service delivery, the speed of AI advancements opens opportunities for providers to implement technologies in new ways.

AI and data analytics can greatly improve efficiencies; however, entities will need to store more data which will require greater levels of utility support to meet the demand. Predictive maintenance and advice by integrated AI could also be manipulated to influence operational activity and societal behaviour.

Robotics and automation bring benefits but may also create new single points of failure that can be exploited if not adequately protected.

The speed of new technology development and implementation has the potential to catch planners by surprise. It is important that risk management plans consider not just new technology but anticipate shorter timeframes for their introduction and identify potential new areas of vulnerability and impact their implementation may introduce.

RISK CONSIDERATIONS FOR EACH SECTOR RELATED TO CYBER / INFORMATION THREATS

COMMUNICATIONS

The widespread adoption of 5G has offered many benefits and created new security challenges. The next generation transition and the need for greater latency and wireless speeds should already be a part of risk planning.

HEALTHCARE AND MEDICAL

The security of patient information and medical research are not aligned with the transition to digitalised record keeping and reliance on outsourced IT services, thus posing concerns around operators' cyber literacy and security practices.

DATA STORAGE OR PROCESSING

Large Language Model or AI processing services require data sector operators to consider how to protect sensitive data they are hosting from being made public.

HIGHER EDUCATION AND RESEARCH

Widespread sharing of research and learning across multiple institutions and different online platforms Is difficult to protect due to vulnerabilities in system security uniformity.

ENERGY

Reliance on industrial control systems and OT, some of which are hosted on dated infrastructure, underpinned by a push toward remote management will likely unearth new vulnerabilities.

SPACE TECHNOLOGY

Increasing dependence on space-based critical services is yielding value for malicious targeting of infrastructure to create the widest impact.

FINANCIAL SERVICES AND MARKETS

The amount and the length of stored personal and financial information potentially leave providers open to greater reputational and operational impact following a cyber breach.

TRANSPORT

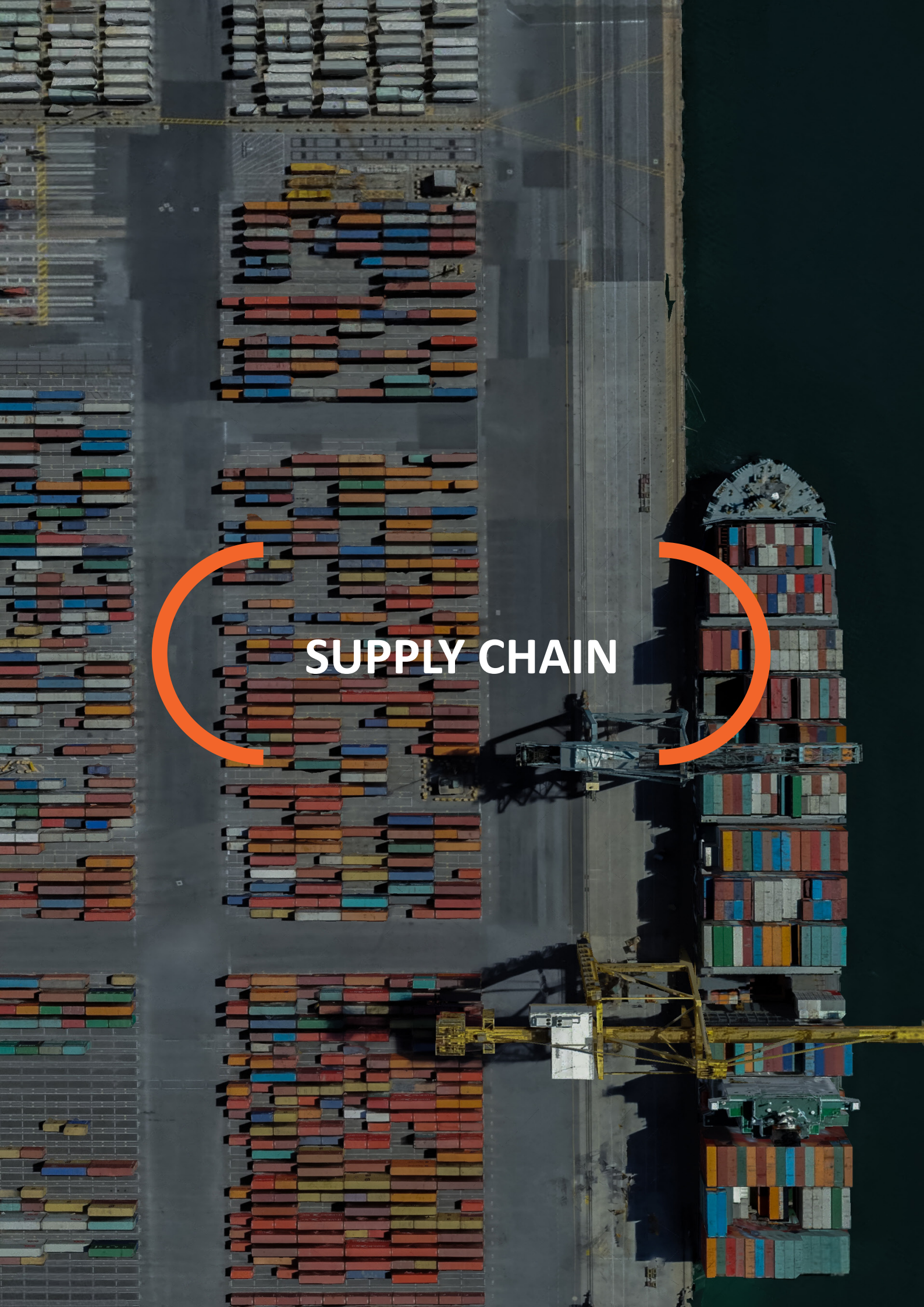
Even small disruptions to major transport control systems can quickly cascade into significant sector and nation-wide economic disruption.

FOOD AND GROCERY

Automated systems across the food production and delivery network allow for multiple points of failure that can have widespread disruptive impacts.

WATER AND SEWERAGE

Disrupting or preventing any level of delivery of critical services required for quality of life creates multi-faceted impacts for the economy and society, no matter the motivation for the attack.


SUPPLY CHAIN

Supply Chain

Australia is reliant on vulnerable international supply chains. Our critical infrastructure relies on internationally-based providers for most of the critical componentry and software. Across most critical infrastructure sectors, vulnerabilities can be easily exposed if adequate contingencies, alternatives or backups are not in place for a full-scale cessation or long-term shortage of critical components from foreign-based suppliers.

Supply chains are increasingly complex. Rather than thinking of a 'chain' as a single line (point A to B to C), supply chains are networks of upstream, downstream and interconnected services, with multiple tiers of suppliers. These expose supply chains to a wide range of potentially disruptive events, across geopolitical, environmental, societal and economic domains.

Long supply chains (distances and number of touchpoints), geographic clustering and inflexibility (i.e. single source supply) all contribute to increased risk of significant supply disruption. Critical infrastructure providers need to consider supply chain-related risk beyond just a disruption to a single provider or to a linear supply line, and consider more holistically vulnerabilities across entire supplier networks.

While the location of manufacturing for semiconductors is slowly diversifying, Taiwan remains the largest supplier. Growing demand for for specialised chips used in emerging technologies, in addition to existing supply requirements, increases vulnerability to a 'by-order' manufacturing market. Australia's limited manufacturing capability increases the length of semiconductor supply chain as we remain reliant on international operators who integrate chips into the end technology.

Over reliance on single-source suppliers or supply lines increases vulnerability for service delivery. Almost every critical infrastructure sector relies to some extent on vulnerable single source supply chains.

Supply chains that are concentrated in single countries, or regions within single countries are highly vulnerable to changes, disruption, malfunction, or sudden demand spikes.

Critical infrastructure sectors are operating in an increasingly frenetic and competitive international supply market. Single source supply chains are highly vulnerable to manufacturers halting or limiting production in response to business needs, domestic policies, geopolitical pressures and nationalist decision making, global shortages, or disruptions to third-party, pre-manufacturing supply chains.

Our critical infrastructure sectors have few contingencies to manage long-term shortage from a single-source supplier. Stockpiles can mask the impact of significant supply disruption, but they cannot fill the gap left by the loss of a sole supplier, nor reduce the risk of long-term shortages.

Workforce supply chains and skilled worker pipelines are under significant pressures. Australia remains limited in its ability to provide the required skilled personnel to fill vital roles in critical infrastructure. Personnel shortages are affecting almost every sector and are likely to continue in the short to medium term.

While strategies are being introduced to manage personnel shortages, any significant events that may worsen shortages will test coping capacity in all sectors, with some unlikely to be fully equipped to respond.

Workforce pressures can also be a catalyst for new operational risk, including personnel functioning in roles with inadequate training or skills, fast-tracking automation or advanced technology without adequate contingency and creating workforce disgruntlement or exodus.

Exposure to increasing numbers of vendors in a global market is an ongoing concern. Critical infrastructure operators are dealing with more vendors that have access to company-sensitive data.

Where vendors also supply critical componentry or technology, reliance on proprietary, advanced or highly specialised technology enhances the criticality of these vendors.

In a global critical infrastructure supply chain, further challenges occur if products and services are purchased by a third party located in a region, or begin to act in a manner, that threatens the national interest.

Access to critical minerals is vital to the development and sustainment of operations across many critical infrastructure sectors. The production of some critical minerals is concentrated in a small number of countries, including a number outside Australia (Fig. 3), and leaves the supply of these minerals to several disruptions, most acutely geopolitical events.

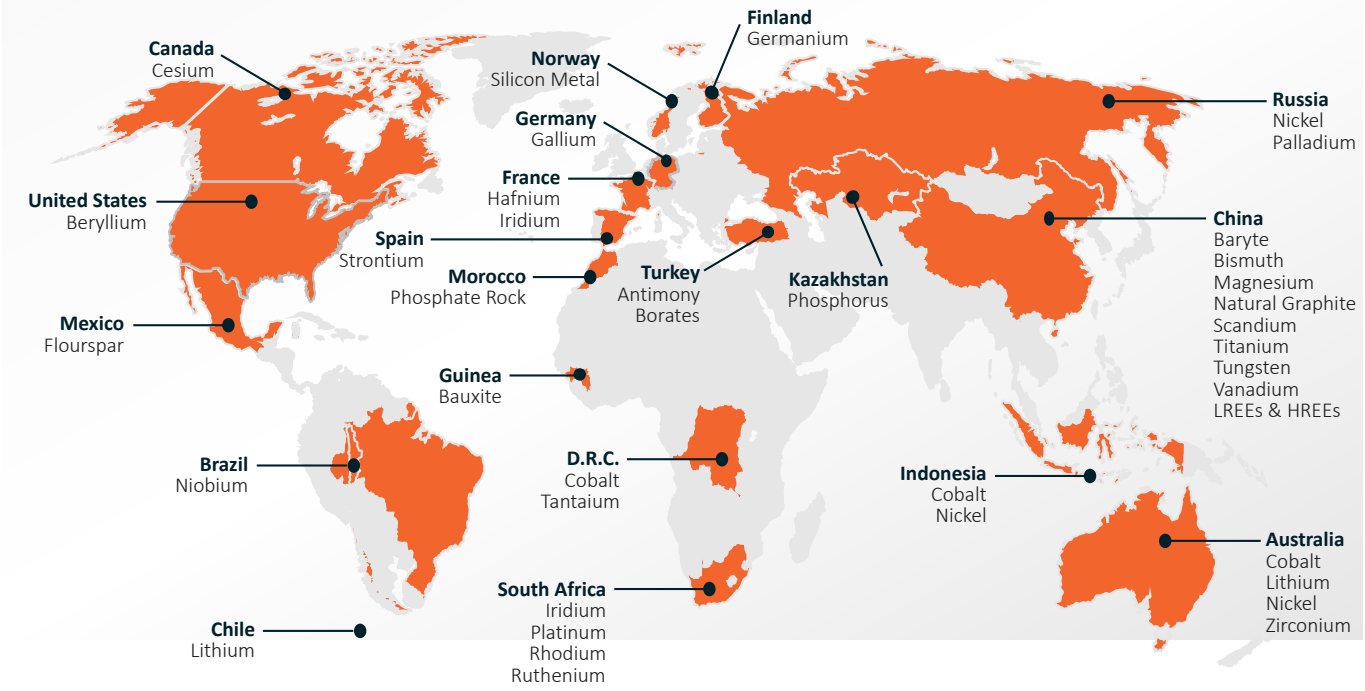
There is a potential for foreign states to use local technology products and service providers as vehicles for conducting foreign interference. Such risks are best identified by understanding who creates the technology, how the technology is used and the impact of the technology within the geopolitical environment.

Failure, acquisition of, or foreign interference from, a vendor with critical intellectual property, original equipment and/or software could be catastrophic to our critical infrastructure operations compromising efforts for greater sovereign control of systems.

Obfuscation of operators along supply chains is challenging. It is very important to understand where critical components and services come from. Shifting and overlapping ownership structures can be used to circumvent international sanctions or be used by actors to gain influence or operational control over critical infrastructure.

Supply chains may be seen as less-secure backdoors into our critical infrastructure networks, and an easier entry point for adversaries to damage or disrupt vital critical infrastructure services. Suppliers accessing valuable systems are attractive targets as they operate with privileged access, or control large sections of a supply chain.

Fig. 3. Map of countries providing critical minerals (source: *GeoERA, European Union)*.



RISK CONSIDERATIONS FOR EACH SECTOR RELATED TO SUPPLY CHAIN HAZARDS

COMMUNICATIONS

Components provided by foreign suppliers may be affected by international sanctions and even if available, Australian communication entities may not be able to purchase needed components.

HEALTHCARE AND MEDICAL

Reliance on international supply lines and resources can have a significant impact seen through labour shortage or shortcomings in critical supplies.

DATA STORAGE OR PROCESSING

Reliance on electronic components sourced globally exposes supply chains to multiple disruptions, including trade sanctions, regional conflict or supply shortages.

HIGHER EDUCATION AND RESEARCH

Market, regulatory and financial risk pressures on student enrolmenty, will challenge higher education institutions to sustain financial health and adequately fund operations.

ENERGY

The average cost of transformers has doubled or tripled since 2020, and supply timeframes have grown over the same period from 3-6 months to around 2 years.

SPACE TECHNOLOGY

The sector relies on internationally-sourced and specialised components and advanced technologies; shortages of these will directly affect the functioning of communication assets.

FINANCIAL SERVICES AND MARKETS

Technology-driven service delivery relies on third-party solutions for corporate functions. This exposes providers to the failure of third parties through maladministration, capability shortcomings, or inadequate security practices.

TRANSPORT

Operators in the transport sector often rely on unique and specialised equipment from very limited sources, which gives rise to various supply-chain risks creating vulnerability for service delivery.

FOOD AND GROCERY

Disrupted supply of chemicals and critical technologies, such as fertilisers and machinery, may restrict crop yields and extent of farmable land.

WATER AND SEWERAGE

Limited supply options for critical water treatment chemicals leave the sector to vulnerable to multiple potential disruptive events leading to a cessation of supply.


PHYSICAL

Physical

Espionage and foreign interference have supplanted terrorism as ASIO's principal national security concern. Espionage and foreign interference targeting Australia's critical infrastructure undermines our national security and sovereignty. Even a small level of activity can have severe consequences which take years to be addressed.

All critical infrastructure providers are legitimate targets for espionage and foreign interference. Our critical infrastructure presents a multi-level espionage target for adversaries. Interest can vary from an intent to obtain critical research and property information, to details on production and service levels, and other information vital to an understanding of how Australia delivers its critical services.

As critical infrastructure operations mature, adversaries will exploit tactics including expanded cyber, human intelligence, or technical collection, to target and infiltrate. The aggregation of open-source data can be highly valuable as a supplement to collection, or to assist with intelligence targeting. This information, when combined with other intelligence collection methods, assist foreign states to gain a more holistic understanding of how Australian delivers critical services.

The terrorist threat is not extinguished, and an attack remains possible. Extremists will seek to generate fear in the community to promote their cause. Disruptive activities against critical infrastructure will continue putting pressure on risk management.

Misinformation and disinformation erodes trust in the delivery of services. Targeting critical infrastructure could be used as a tactic to breakdown confidence in the government's ability to deliver services, or even to demonstrate foreign state power to influence public support for conflict or support of allies.

The use of misinformation and disinformation is extending beyond social media, and the amplification of untruths can be difficult to mitigate and contain. Direct targeting of issue-motivated groups is also a tactic to influence human behaviour, spurning protest, activism or harmful actions.

Misinformation. False information is shared, but the cause of harm is not intentional.

Disinformation. False information is willingly shared with the intent to cause harm.

Malinformation. Legitimate information is shared to cause harm by making it public from a private source.

Grey zone tactics are an avenue for physical attack. Physical grey zone attacks, considered as activity designed to coerce a target while seeking to avoid military conflict, remain a threat to critical infrastructure.

Grey zone conflict can provide ambiguity as to the source of any attack. Even isolated impacts against specific infrastructure assets may have cascading effects across critical infrastructure sectors. As such, it is important for providers to have a clear understanding of both upstream and downstream dependencies.

Intentional physical grey zone attacks can create confusion over whether the incident is malicious or technical. Infrastructure located in difficult to reach locations are at heightened risk for this style of incident.

Well-resourced actors could target undersea cables or submarine cable landing stations that connect Australia to the rest of the world. Across the space domain, a satellite could be intentionally diverted from its orbit and redirected on a collision course with another satellite.

Post-pandemic corporate activity is increasing the touch points for foreign government contact and influence operations. Australia's corporate travel is again at a high level following the period of COVID-19 travel limitations. Attendances at conferences, trade shows and other business-related travel provide increased opportunities for contact with foreign state actors.

Critical infrastructure providers must remain vigilant in educating personnel travelling or attending conferences about foreign contact risk and the need for contact reporting.

Corporate IT hardware and personal devices need to be appropriately protected and used in accordance with safe practices for device security.

The Australian Government is collaborating with businesses and institutions to protect against such compromise to help preserve our sovereign capability and commercial and scientific advantage. ASIO's NITRO Portal is an essential element of collaborative efforts between the Australian Government, business and academia to prevent the compromise of privileged information.

LinkedIn remains a cost-effective and rich source of targeting for foreign contact. Over 2023, there have been several high-profile cases in Australia and overseas of business travellers being approached and ultimately recruited to provide information to foreign states.

Issue-motivated activity has the potential to cause disproportionate impacts. Small-scale and specific targeting of strategic critical infrastructure by issue-motivated activity has an ability to result in wide-scale and cross-sector disruption. Such activity can range from infrastructure sabotage, public influence operations, illegal protest and blockading, which can all significantly disrupt or even halt the delivery of services.

In 2023, critical port operations in Sydney, Melbourne and Newcastle experienced varying degrees of disruption from issue-motivated protest activity. Ports are a critical dependency to most sectors and cross-sector recovery as a result of even small-scale disruptive incidents can persist long after the incident has been resolved.

Foreign influence of boards, standards bodies and industry bodies. Key regulatory functions, such as company boards, standards and industry bodies, can have a profound impact on the way critical services are delivered in the interest of our national security.

External influence operations may attempt to manipulate the way company boards and regulatory bodies function and disrupt or force outcomes unfavourable to Australia.

Regulatory compliance is especially important in industries with strong compliance oversight, such as financial services and healthcare, and sectors where data protection, cybersecurity, and consumer privacy are critical to business continuity and legally compliant operations. Complacency over threats to regulatory bodies can lead to limited regulatory compliance focus and diminished security.

Physical security measures are are also a key enabler for cyber security measures. Physical impacts may result from a cyber or information threat. Similarly, physical threats or access to sensitive areas could facilitate a cyber incident. Remote access to operational technology and industrial control system devices controlling critical infrastructure could be affected by an outage to communications infrastructure.

RISK CONSIDERATIONS FOR EACH SECTOR RELATED TO PHYSICAL THREATS

COMMUNICATIONS

Foreign ownership in Australia's communication networks may be subject to interference from foreign adversaries, using access or coercion to gain access to networks or to transmitted and stored data.

DATA STORAGE OR PROCESSING

Actors with intent to cause widespread harm may target the utility supply of water, electricity or subterranean communication cabling to a data centre.

ENERGY

Foreign ownership in Australia's energy generation and transmission may be subject to interference from foreign adversaries, using access or coercion to cause disruptions.

FINANCIAL SERVICES AND MARKETS

Criminal activity can cause damage through fraud, insider trading or stock market manipulation. These criminal activities can have broader consequences such as reputational damage and loss of income.

FOOD AND GROCERY

Foreign ownership in Australia's food and grocery production and distribution, and agricultural land, may be subject to interference from foreign adversaries, using access or coercion to cause disruptions.

HEALTHCARE AND MEDICAL

A malicious attack resulting in a mass casualty event could overwhelm stretched hospital and health networks.

HIGHER EDUCATION AND RESEARCH

Researchers with high-valued expertise and those working on government research and development remain an attractive target for espionage, even more so when travelling internationally for work.

SPACE TECHNOLOGY

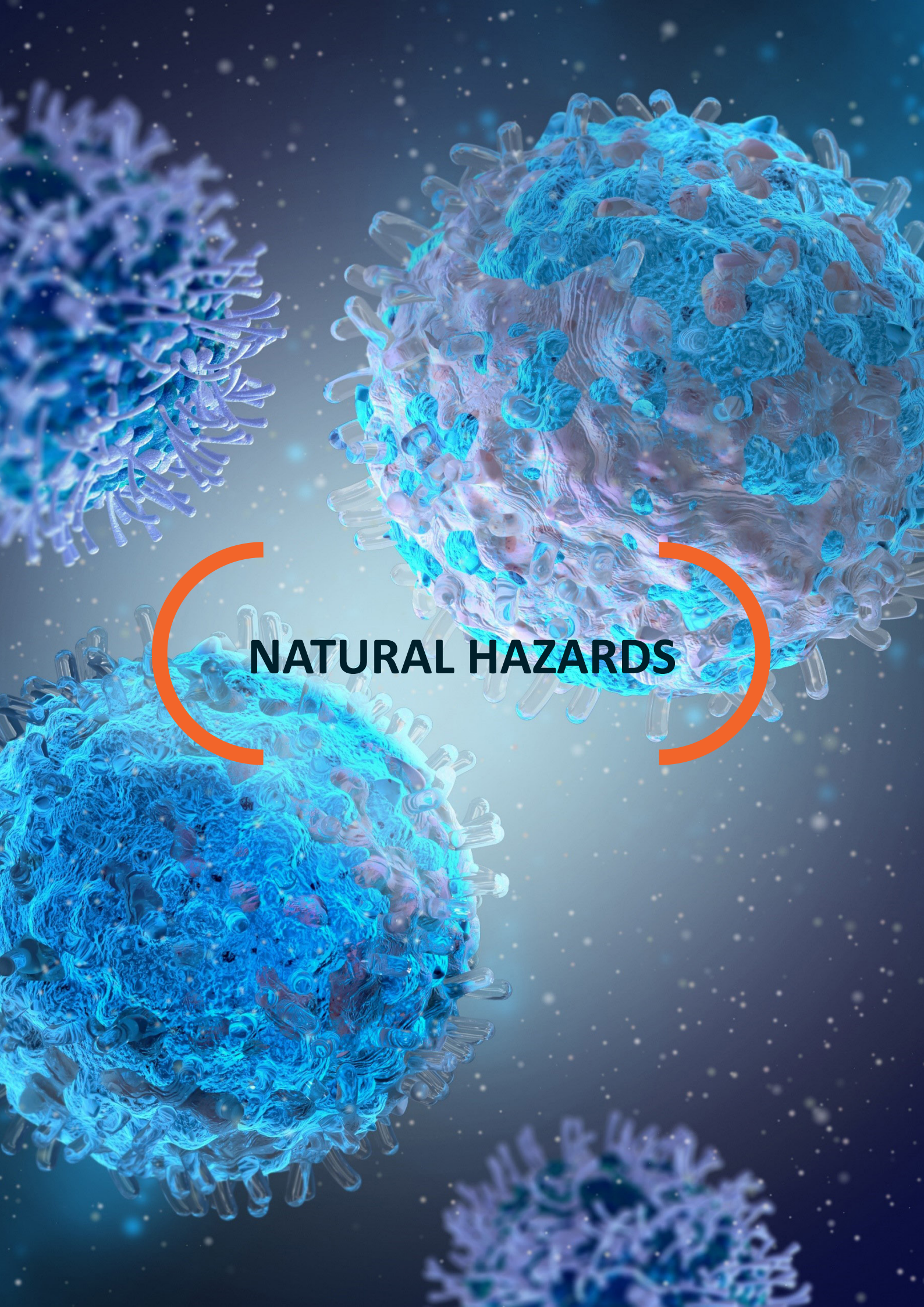
Space debris and pollution pose a risk of damaging spacecraft and satellites in orbit. Major damage could affect the functioning of the asset and compromise its availability, integrity and reliability to transmit data.

TRANSPORT

Equipment used at Australian ports or by transport networks may include inherent vulnerabilities when sourcing is limited to certain countries or vendors.

WATER AND SEWERAGE

Groups that seek to make political statements, particularly ethical, through unlawful means may intentionally damage or disrupt port, rail, road and other water/transport/supply chain infrastructure necessary for the sector.



NATURAL HAZARDS

Natural Hazards

Changes in the Earth's climate are bringing more frequent and intense natural hazards. As natural hazards are increasingly severe and recoveries more difficult, reliance on historical precedent for risk management has become inadequate.

In addition, such unpredictability means that climate-related risks may go unnoticed. Our critical infrastructure is located across environmental locations that are subject to different natural hazards. Geographical shifts in the occurrence of natural disasters are also likely to challenge critical infrastructure providers that may be otherwise unfamiliar with preparing, responding to, and recovering from certain types of natural disasters.

Flood and extreme storms, including cyclones, constitute natural hazards that cause the greatest financial loss for our economy. As much of Australia is bushfire-prone, including areas hosting some of our most significant infrastructure, the loss of which can place pressure on many more critical services.

The number and intensity of annual severe weather events is increasing. Climate extremes already affect many facets of Australian society including health, soil and water, agriculture, infrastructure, energy security and financial security, posing significant risks to the global and Australian economy.

Australia will face more climate extremes in the future. Australia experienced a year of record-breaking weather events in 2022 with rain and flooding overshadowing all other natural hazard events. Second and third consecutive La Niña events have dominated the climate across eastern Australia; and contributed to persistent, heavy rainfall breaking multiple daily, monthly and yearly flood and rainfall records.

Space weather is a complex natural hazard with potentially significant consequences for critical infrastructure. Although space weather (Fig. 4) is a widely recognised risk, its potential impact on modern critical infrastructure, society and the economy remains uncertain and untested. Our critical infrastructure therefore has limited understanding of the figurative boundaries for an extreme space weather event; and awareness and preparedness are unequally spread across sectors and providers.

More extreme variants of space weather happens more frequently and with increased intensity around the solar maximum and its proceeding decline; however, strong space weather events have been observed at other periods along the solar cycle.

Much of our modern technology has yet to experience a direct, extreme space weather event, including key assets in some vulnerable domains (i.e. lower earth orbit satellites) that have yet to experience a solar maximum period.

Natural hazards do not occur in a vacuum and can have far-reaching upstream and downstream impacts. Continued changes to our climate may result in more concurrent or consecutive disasters that all require attention, resulting in longer periods of disruption.

The increasing interdependencies between critical infrastructure sectors have created an environment where impacts in one sector can easily expand to others. Most damage from extreme weather events can be readily repaired. However, there may be connected and dependent critical infrastructure and supporting utilities for which even a short outage is significant.

Construction standards and utility planning can mitigate the impacts of natural hazards. Critical infrastructure is highly vulnerable to, and a major casualty of, natural disasters. Repairing or replacing infrastructure assets after a disaster is often difficult and costly.

Our future high quality and resilient critical infrastructure needs to be defined by its ability to withstand more extreme and regular changes in climate. Resilient infrastructure also functions in supporting communities to withstand, respond to and recover from natural disasters. However, even the most severe events are likely to exceed business continuity plans and design standards.

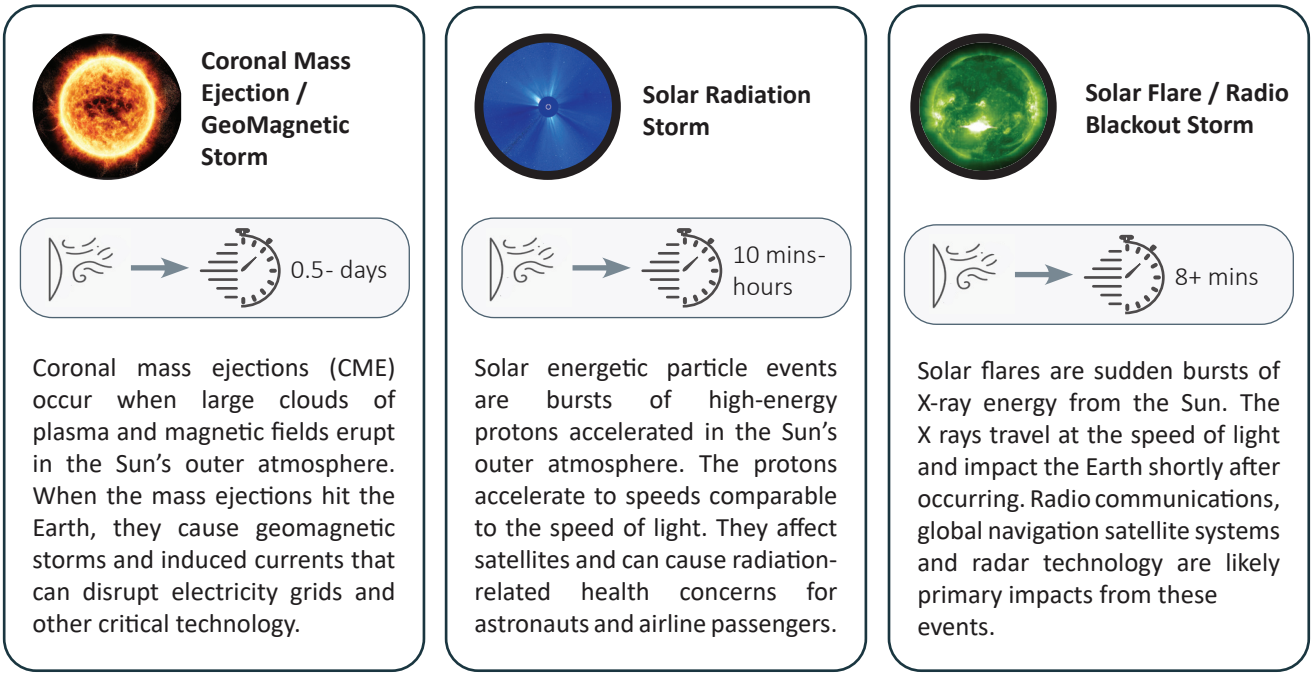
The changing nature of natural hazards means critical infrastructure projects remain vulnerable to uncertainties around risk management, over which there are varied levels of control. Decision-makers should integrate a risk assessment requirement in project proposals to ensure disaster exposure, asset vulnerabilities and opportunities for hazard prevention or mitigation are identified from the outset.

Global pandemics are exposing vulnerabilities in preparedness under modern socio-economic systems. COVID-19 highlighted how quickly an outbreak can spread globally, threatening the stability and security of critical infrastructure networks and altering the expectations of society around what is needed from critical infrastructure services, particularly for those involved in frontline delivery.

Changing land use patterns and climate effects are also creating new interactions between humans and wild animals, enhancing the risk of widespread zoonotic outbreaks. Zoonotic diseases are more common in South-East Asia and Indo-Pacific regions, and the threat of an outbreak reaching Australia is increasingly likely.

As we recover from the shock of COVID-19, a new global pandemic or multiple, concurrent domestic outbreaks of diseases domestically are likely to overwhelm already stretched systems.

Fig. 4. Summary of the three key space weather events impacting critical infrastructure, including transit time from event to Earth impact.



RISK CONSIDERATIONS FOR EACH SECTOR RELATED TO NATURAL HAZARDS

COMMUNICATIONS

Bushfire hazards present an extant risk to the delivery of telecommunication services. During the emergency response situations, any loss of ground-based communication infrastructure increases reliance and importance of other services.

HEALTHCARE AND MEDICAL

Severe weather has rendered hospitals inoperable or inaccessible, prevented emergency services from reaching people, and threatened domestic supply chains on which critical medicines relies.

DATA STORAGE OR PROCESSING

Concurrent, severe weather events can test the capacity of utility supply to data centres to ensure continuous and uninterrupted supply of energy, cooling and communication.

HIGHER EDUCATION AND RESEARCH

Pandemics have shown their potential to greatly alter the functioning of society, increasing the need for remote learning and collaboration, at times over less-than-secure conferencing. This type of disruption may have wide-reaching implications for the Australian economy.

ENERGY

Damaging winds can cause a failure of electricity transmission and its hosting infrastructure across wide geographic footprints.

SPACE TECHNOLOGY

Space-based assets remain exposed to hazards from space weather events. Previous events have caused failures in satellites and critical infrastructure networks, which are increasingly more interconnected and technologically complex.

FINANCIAL SERVICES AND MARKETS

Increasing numbers of extreme weather events, particularly when occurring close together and impacting populated areas, can pressure the ability of insurance entities in providing and sustaining services to all aspects of society.

TRANSPORT

Flooding has repeatedly caused significant impact on road and rail infrastructure. The impact of this disruption, particularly in high-traffic regions, causes challenges for the sector in the delivery services on which other infrastructure sectors rely.

FOOD AND GROCERY

Ongoing heatwaves over large parts of Australia are one of the most significant natural hazards and can negatively impact agriculture ecosystems and affect their ability to provide consistent food production.

WATER AND SEWERAGE

Bulk water catchments are vulnerable to contamination from bushfires or from fire retardants that are dropped in bushfire affected areas.


PERSONNEL

Personnel

Personnel with insider access are an enduring point of vulnerability. Multiple risk-related events can and are aligned to actions from an insider threat. This may include malicious, negligent, or unwitting acts by individuals with legitimate access and privileged knowledge. Such acts lead to impacts that compromise the proper function of, or cause significant damage to critical assets and services.

Determining the level of insider threat and vulnerability is challenging as insider activity leading to harm can be indistinguishable from legitimate access or activity.

Connectivity between work and personal devices has increased as a result of a growing trend toward working from home and flexible arrangements. This connectivity may reduce the detectability and overall difficulty for a trusted insider to remove local data or provide access to a third party.

Critical infrastructure sectors often operate at a high tempo with increased turnover or significant staff shortages. Such trends may create vulnerabilities through a lack of workplace loyalty, or staff accessing sensitive information without appropriate security clearances, background checks or information handling knowledge.

Under the SOCI Act 2018, responsible entities must establish and maintain a process or system in their CIRMP to manage the access of critical workers and minimise or eliminate malicious or negligent employee or contractor activity. This may include a background check conducted under the AusCheck scheme or other measure.

Trusted insiders, regardless of intent, are a significant threat to any critical infrastructure sector. Insiders can deliberately disclose sensitive or confidential information to third parties, manipulate systems and networks to harm an organisation, or be recruited by foreign intelligence services to undermine the current and future capabilities of Australia's critical infrastructure service delivery. 'Dark web' job advertisements targeting "disgruntled employees" are being used as a recruitment tool as more and more threat actors acknowledge the value of exploiting insider access.

Monetary gain from commercially sensitive research is a strong motivator for trusted insiders. Likewise, disgruntled workers may consider damaging the operations of a sector or tarnishing its reputation.

Collectively, insiders are one of the most attractive targets for malicious foreign actors. Recruited insiders working under the direction of foreign intelligence services can cause significant harm to our national security and can undermine the current and future capabilities of our critical infrastructure. This includes witting insiders who understand what they are doing and why, and unwitting insiders who are manipulated without their knowledge. Malicious actors could also pre-position people to be hired into specific roles.

Increased leaking of classified and sensitive information through chat forum platforms. Over the last two years, several incidents on private chat forums such as Discord and War Thunder platforms, have seen classified or sensitive information leaked, in most cases by individuals with insider and often legitimate access to information.

These types of leaks have varying drivers for intent, although some are perpetrated by a witting insider, perhaps driven by a need to show off access or to prove a point of argument. This trend will require expanded employee online activity management by entities, beyond traditional social media usage.

RISK CONSIDERATIONS FOR EACH SECTOR RELATED TO PERSONNEL THREATS

COMMUNICATIONS

Deliberate disclosure of privileged information or manipulation of knowledge of technology with the intent to cause harm presents greater challenges than leaked personal identification information.

HEALTHCARE AND MEDICAL

Continued staff shortages are putting pressure on the delivery of health services exposing providers to potential workforce disgruntlement and risk-motivated malicious activity.

DATA STORAGE OR PROCESSING

Data centres invest heavily in physical security with leading access control measures. However, centres remain exposed to insiders who may have both legitimate access and technical knowledge to cause harm.

HIGHER EDUCATION AND RESEARCH

Foreign recruitment of research, academic or other administrative personnel could result in the theft of sensitive research or other intellectual property.

ENERGY

Hazards, such as an accidental industrial incident can cause significant risk for an entity. For the Energy Sector, an incident such as an improperly controlled critical system could result in operational failure and flow-on effects to the grid.

SPACE TECHNOLOGY

Individual technical actions that result in an inoperable or improperly controlled satellite could lead to an accidental collision between satellites, creating space debris, accentuating risk to satellite operations.

FINANCIAL SERVICES AND MARKETS

An individual with inside knowledge and intent has the capability to deliberately disclose privileged information, circumvent regulatory controls or manipulate technology to cause harm.

TRANSPORT

Insiders with access to secure areas that interact with the nation's global trade and immigration points can create risk scenarios that threaten the integrity of Australia's border.

FOOD AND GROCERY

Product tampering on food or other goods that are distributed nationally can create sector-wide reputational risk for the trust in Australian produced goods.

WATER AND SEWERAGE

A malicious of unwitting contamination of water or waste treatment can create lengthy disruption to the provision of safe water or result in mass discharge of wastewater in urban or at-risk environments.

LOOKING AHEAD

Looking Ahead

Identifying trends and technology drivers and their impact on risk can be challenging, as trends interact in unpredictable ways, with potential profound consequences.

The following areas of risk are possible domestic changes or trends that could impact the risk profile of our critical infrastructure entities.

Increasing pace of technological advancement and implementation. History suggests that society is quicker to see the upside of new technologies than their downside. More often than not, policy plays catch up to adaptation of new technology with a lack of appropriate regulation creating new vulnerabilities.

The already increasing use of AI, the maturity of IoT and the onset of 6G technologies have shown their value to critical infrastructure and will continue to be adopted into operations in coming years.

It is difficult to predict how new technologies will pose any new risks, particularly as they advance to the point of integration into aspects of societal and commercial life. Commensurately, it is also very difficult to plan and build resilience.

At a minimum, critical infrastructure providers and governments need to consider the potential impacts of new technologies and their implementation into existing operations, including how they will interact with extant technologies and what potential vulnerabilities they may create or exacerbate.

Ongoing supply chain disruption, escalation in costs and construction workforce challenges will pressure infrastructure delivery. Severe labour shortages and supply chain disruptions are causing significant delays and exorbitant cost increases for construction materials, impacting on an industry already struggling with low productivity. Increasing supply chain costs, high global rates of inflation, and longer waiting times for equipment and material result in additional burdens on delivery timeframes for Australian companies involved in large-scale infrastructure projects. While pressures on supply chains have eased slightly, our limited sovereign sustainment capabilities will continue to pressure delivery of these large-scale infrastructure projects.

Any change to workforce shortages in the short to medium term is unlikely. Staffing shortages across all critical infrastructure sectors are likely to worsen over the next 12-36 months, with regional services expected to be impacted most acutely. Organisations continue to rely on inadequately skilled personnel, further exacerbating operational risk and personnel disgruntlement.

El Niño weather pattern to commence a trend to more severe drier conditions. El Niño weather pattern is likely to begin a path that will put pressure on water availability and create more vulnerable environments exposed to severe natural hazard, especially if drier weather patterns continue over a number of years.

Approaching solar maximum towards the end of 2024. The 'solar cycle' is a cycle of solar activity that fluctuates over approximately 11 years. This cycle begins at a solar minimum, which typically correlates with lower solar activity and few sunspots (indicators of activity). As the cycle continues, sunspots increase along with other activity, including solar flares, coronal holes and coronal mass ejections. The top of the cycle, solar maximum, sees solar activity peak, then gradually decline, returning to solar minimum. Critical infrastructure operators should consider direct and indirect impacts from extreme space weather events as part of their business continuity planning.

No let up to cyber disruptions! Successful penetration of Australia's corporate systems is unlikely to abate in the short term with increasing potential for bigger and more disruptive information breaches. Critical infrastructure providers must ensure a fatigue of messaging and complacency does not hinder resilience and cyber security efforts.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE