Australian National University

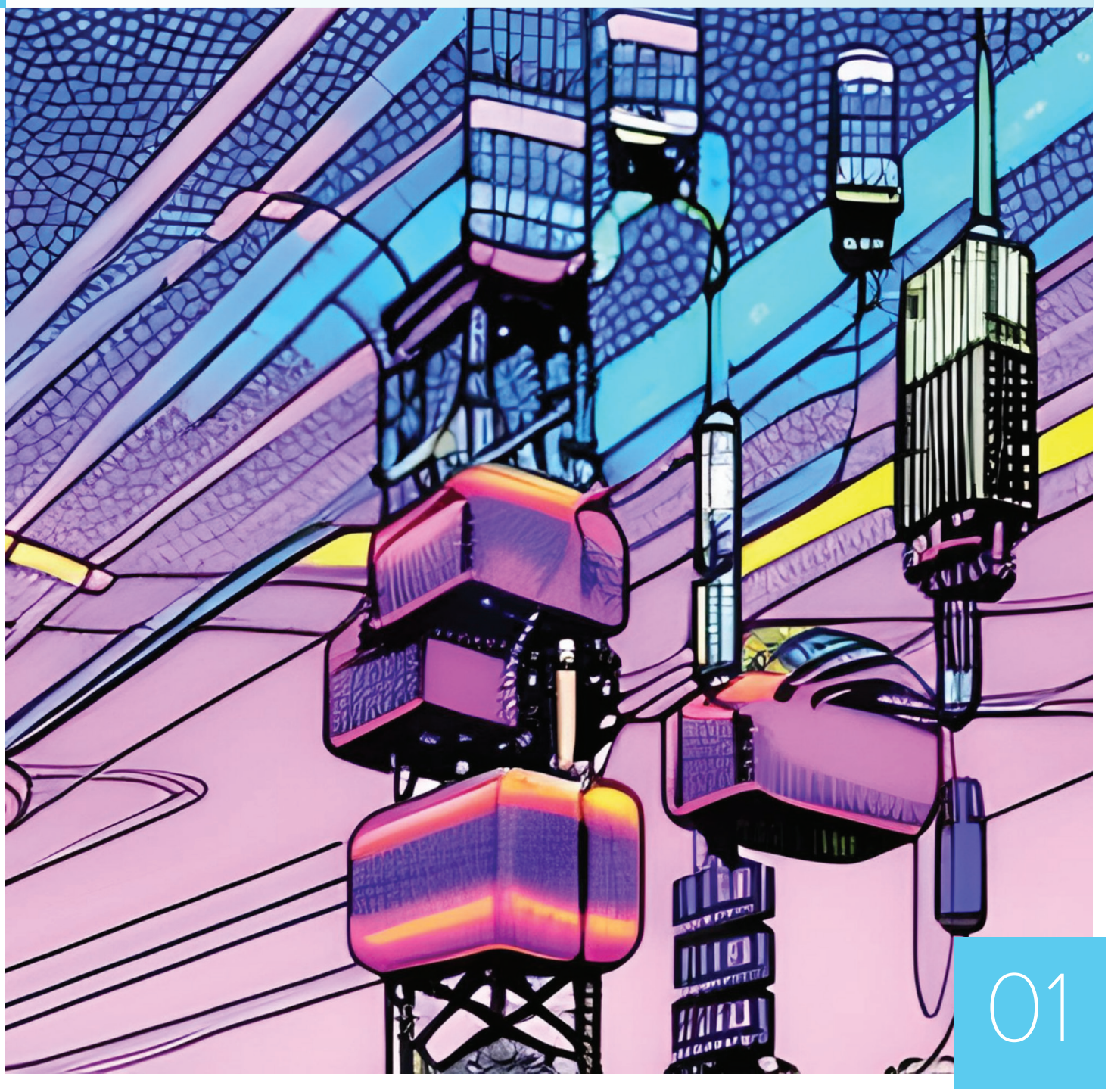
TECH POLICY DESIGN CENTRE

AUGUST 2023

Telecommunications Risk and Resilience Profile

Pestle and Gap Analysis

> We often think about national resilience at times of crisis or conflict. However, the foundations for resilience are built with every decision we make before a crisis begins to unfold.
>
> – Gill Savage[1]



About the Tech Policy Design Centre

The Tech Policy Design Centre (TPDC) is a nonpartisan, independent research organisation at the Australian National University. TPDC's mission is to develop fit-for-purpose tech policy frameworks to shape technology for the long-term benefit of humanity. We work to mature the tech-governance ecosystem in collaboration with industry, government, civil society, and academia.

Independence Statement

Our work is made possible by the generous support of external funders from government, industry, and civil society philanthropy. Our research aligns with ANU's Statement on Academic Freedom. In all instances, TPDC retains full independence over our research and complete editorial discretion for outputs, reports, and recommendations.

Authors

Dr Huon Curtis, Senior Research Fellow, ANU Tech Policy Design Centre
Chloe Harpley, Project Manager, Department of Infrastructure, Transport, Regional Development, Communications and the Arts
With invaluable support from Professor Johanna Weave and James Jackson, Research Assistant, ANU Tech Policy Design Centre

Acknowledgements

The TPDC acknowledges the Ngunnawal and Ngambri people, who are the Traditional Owners of the land upon which this report was prepared. We pay our respects to their elders, past, present, and emerging.

This report was funded by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts. The project will culminate in a Telecommunications Sector Risk and Resilience Profile, to be released in 2024.

TPDC thanks all who contributed to this work including: the project's expert group, Alexander Osbourne, Cameron Scott, Carolyn Phiddian, Colin Muller, Craig Smith, Dave O'Loan, Dan Weis, David Haigh, Ebony Aitken, Elise Ball, Dr Gareth Downing, Gill Savage, Dr Holly Randell-Moon, Jamie Morse, Jason Duerden, Jeff Whitton, Kirsty McKinnon, Laurence Plant, Luke Coleman, Michelle Phillips, Min Livanidis, Narelle Clark, Dr Paul Barnes, Professor Ryan Ko, Stephen Farrugia, Fred Fernandes, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, and the Department of Home Affairs; and all of our survey participants.

The report's cover and image are AI-generated images from Canva, while the layout was created by the Black Bear Creative team.

Citation

Curtis, H. and Harpley, C. 2023, Telecommunications Sector Risk and Resilience Profile: PESTLE and Gap Analysis, ANU Tech Policy Design Centre, Canberra, ACT.

Contact

Tech Policy Design Centre
5 Fellows Road, College of Law
The Australian National University Canberra ACT 2601, Australia
techpolicydesign@anu.edu.au

CRICOS Provider: 00120C

Australian National University

TECH POLICY DESIGN CENTRE

Table of Contents

1. Objectives and overview

The objectives of the project are to develop a sector-wide telecommunications risk and resilience profile taking an all-hazards approach, and to provide an independent evidence base for future policy decisions.

The project focuses on risk and resilience of the telecommunications sector in areas of existing connectivity and draws on the collective expertise of government, industry, utility providers, emergency services, the disaster management community, and academia.

Over five stages, the project will:

1. Establish the scope and context for a telecommunications sector risk and resilience profile.
2. Identify sources of risk.
3. Analyse risk including vulnerabilities, hazards, threats, and extreme events that have led, or may lead to, risk exposure within the telecommunications sector. This process will include evaluating cascading, compounding, interacting and interconnected risk.
4. Identify options for treating risk that will strengthen the overall resilience of the telecommunications sector.
5. Synthesise all stages into the final Telecommunications Sector Risk and Resilience Profile.

This report details the outcomes of stage one of the project.

2. Establishing scope and context

The establish scope and context, the research team undertook an initial stakeholder questionnaire (see Annex D) supplemented by desk research and qualitative data gathered via interviews with leading telecommunications, technology, risk and resilience experts, industry, and government stakeholders.

Two clear gaps were identified:

- The gap of an appropriate methodology that combines considerations of risk and resilience.
- Gaps in clarity of terminology around 'risk' and 'resilience'.

To address these gaps, this paper outlines international frameworks and guidelines, drawing on them to establish a sectoral risk and resilience methodology.

Sector Risk Profiling (SRP) is a methodology that has been used to develop a risk picture for other sectors, such as the Australian aviation sector.[2] However, this methodology does not incorporate 'resilience.'

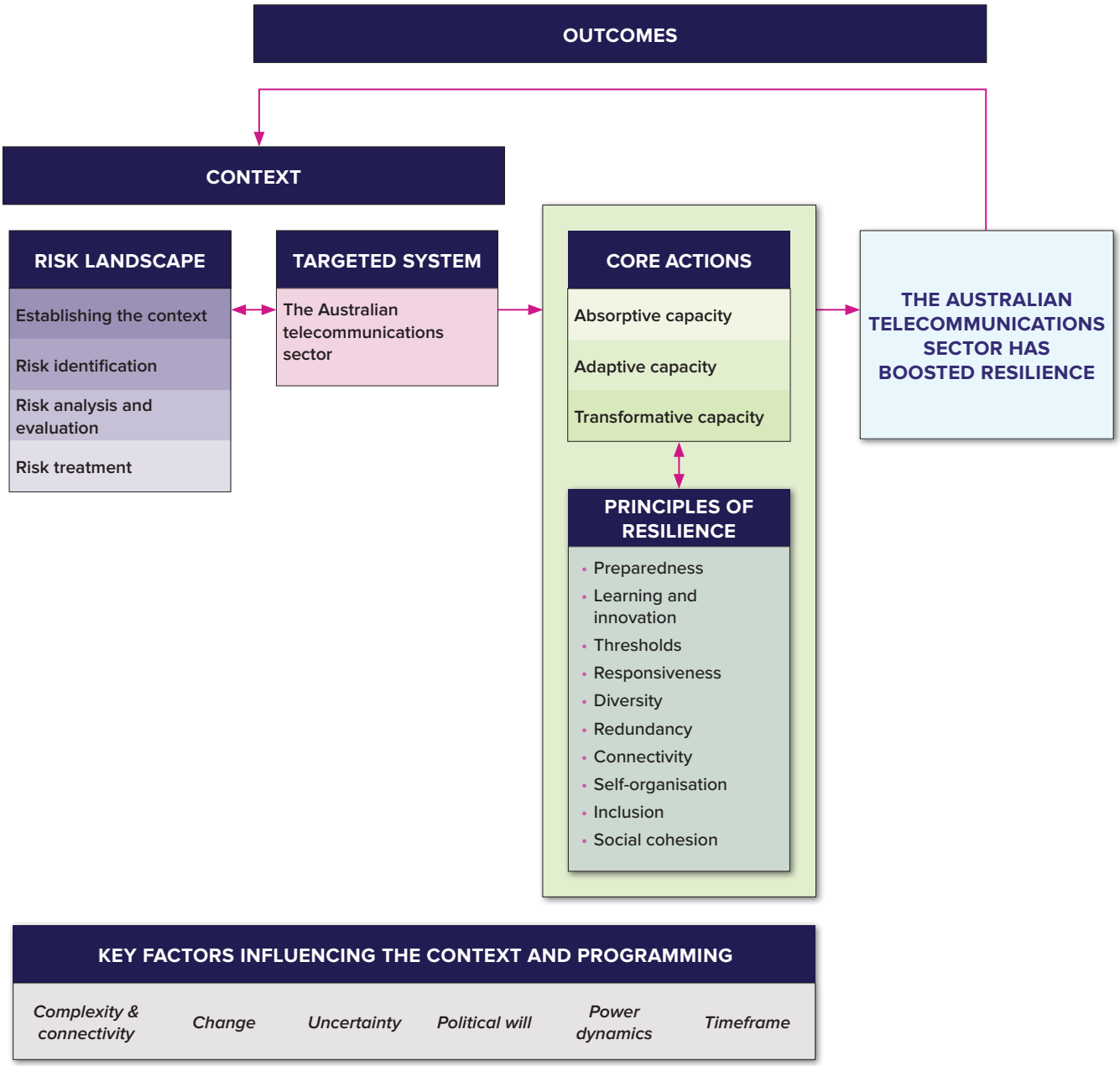
The Organisation for Economic Co-operation and Development (OECD)'s *Guidelines for Resilience Systems Analysis* offers a way to incorporate both concepts (see Figure 1).[3] Resilience systems analysis enhances traditional risk management approaches by addressing complexity and interdependency. It goes beyond 'known risks' to account for uncertainty, change, and long-term trends.[4]

The OECD approach provides a conceptual framework and methodology that asks four key questions when setting the scope of analysis. These form the primary headings for this report.

- Resilience of what system?
- Resilience of who?
- Resilience to what source or potential for disruption? (PESTLE analysis of all-hazards risk approach)
- Resilience over what timeframe?

This paper draws on three primary sources to develop definitions and terminology for the rest of the project: *ISO31000:2018 Risk Management – Guidelines, the ISO/IEC 31010:2019 - Risk management - Risk assessment techniques, and the ISO/IEC27000-family – Information security management.*

Figure 1: OECD systems analysis map



Source: adapted from OECD Guidelines for Resilience Analysis (2014)

3. Defining risk and resilience

Working definition of risk

Risk in the telecommunication sector is the:

Likelihood of a disturbance causing impacts to the viability of the assets and services in the telecommunications sector. Assessments of likelihood and consequence are impacted by degrees of uncertainty.

Risk and resilience are two fundamentally different concepts but are often conflated as one and the same. The working definition of risk reflects international standards and applies them to the networked systems that are the concern of this project.

Background

In the enterprise risk management context, the ISO31000:2018 defines risk as 'the effect of uncertainty on objectives.'[5] However, the ISO27000:2018 standard provides more precise notes to risk and uncertainty in information technology environments.[6] It notes that an effect can be a positive or negative deviation and that uncertainty is both related to a state of incomplete information or knowledge and a calculation of the impacts of an event. The notes explain that:

- *Risk is* the effect of uncertainty on objectives, *where*
- *Effect* is a deviation (positive or negative) from the expected;
- *Objectives* can have different aspects (e.g. financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process.
- Risk is often expressed in terms of a combination of a consequence of an event (including changes in circumstances) and the associated likelihood of occurrence.
- *Uncertainty* is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

The ISO27000:2018 guidelines also outline the definitions and appropriate terminology of related concepts of risk management including risk identification, analysis, assessment, criteria, and evaluation and acceptance.

A risk assessment process is the overall process of risk identification, analysis and evaluation.

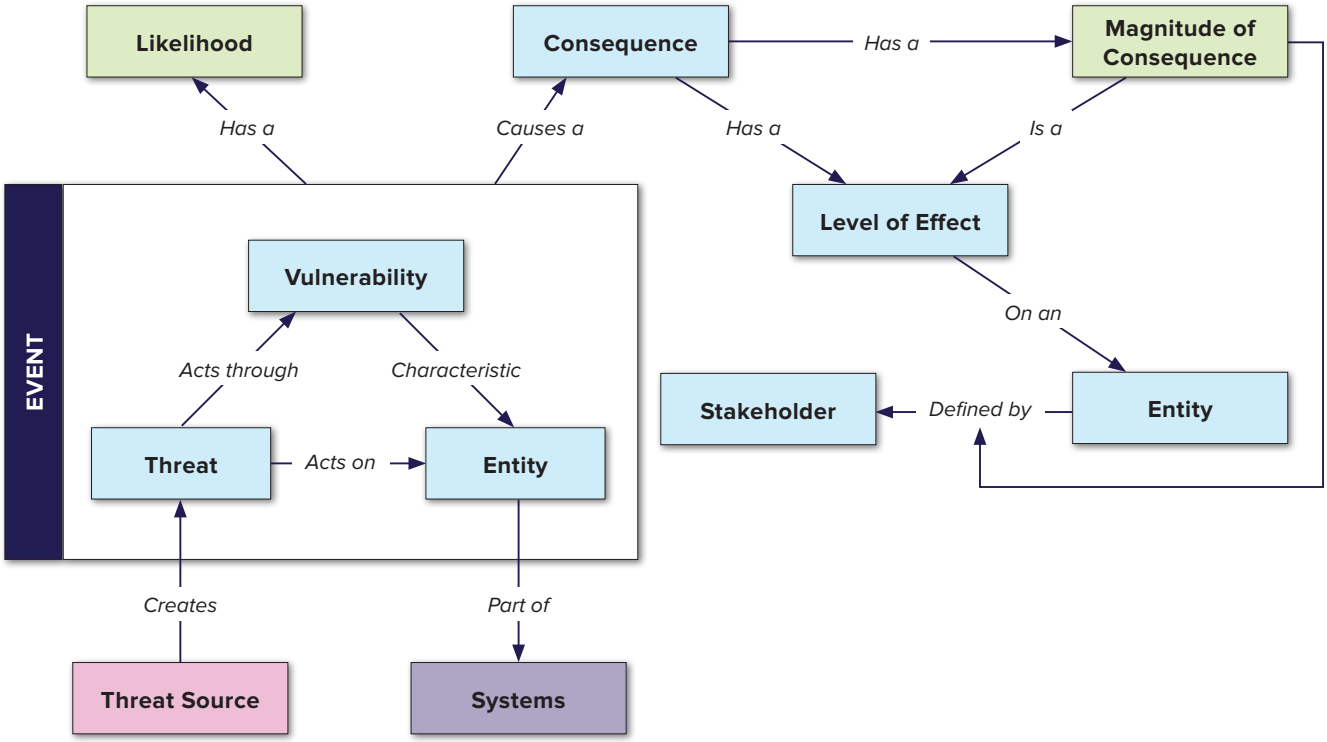
- Identification is the process of finding, recognizing and describing risk (e.g. their sources, causes and potential consequences).
- Analysis is the process to comprehend the nature of risk and to determine the level of risk.
- Evaluation compares the results of analysis with risk criteria to determine whether the risk, and or/its magnitude is acceptable or tolerable.

Risk-based approaches can be helpful to understand how a specific threat (i.e., potential cause of an unwanted incident that may result in harm to a system or organisation) may impact a system. These approaches can lack the characteristic of reviewing how linkages and interdependencies with other systems leave one vulnerable to cascading failure and systemic threat.[7]

Figure 2 outlines the terminology that this project has adopted and shows that the risk landscape is characterised by threat sources that can initiate threats, which in turn manifest as events in entities in a system by exploiting an existing vulnerability.

Further notes to relevant definitions drawing on ISO27000:2018 are provided in Annex A.

Figure 2: Factors in risk



Source: Branagan (2012)

Working definition of resilience

Resilience in the telecommunication sector is:

The capacity to anticipate, absorb, recover, adapt and transform from disruptive events by identifying, understanding, and analysing interdependencies to clarify types of failure, and necessary response behaviour.

This may involve boosting infrastructure characteristics (management and organisational, safety, social, sustainability, technical and financial) and changing environmental factors (e.g. public policy, health and safety) to provide an essential, or critical, service to the nation.

The working definition incorporates definitions from academic, policy and practitioner literature and orients them to the context of critical infrastructure.

Background

Resilience has various definitions and in general terms refers to 'before, during and after' an unwanted event or disruption.[8] The time dimension covers the whole crisis management cycle.[9]

OECD guidance defines resilience as: "the ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty."[10]

The United States' National Academy of Science defines resilience in relation to disasters as: "the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions."[11]

However, this project needs to be oriented around 'risk and resilience' in the context of critical infrastructures with a focus on telecommunications.

Critical infrastructures are "highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies (so-called "cyber-based systems")," according to one of the most highly cited works (see Figure 3).[12] However, analysis of the effects of the interdependent infrastructure systems is relatively sparse and requires some methodological novelty.[13]

Interconnected systems need to maintain functionality, and to understand this a concept is needed to accounts for normal stressors to more severe disruption. The concept of 'state of operation' accounts for: "a continuum of different behaviours during normal conditions (which can vary from peak to off-peak conditions) during times of severe stress or disruption, or during times when repair and restoration activities."

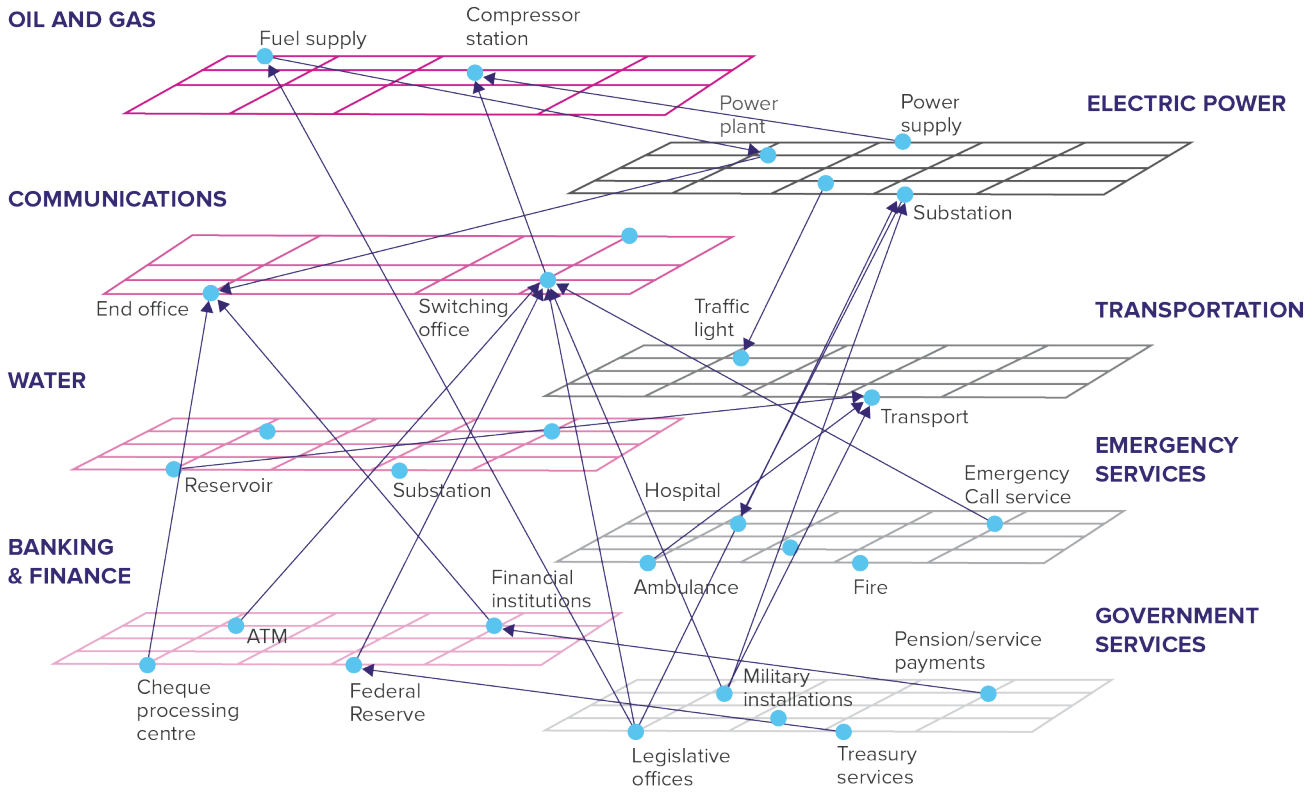
This continuum can range from: "Optimal design operation to complete failure with a total loss of service to all users (including all dependent infrastructures). Under certain conditions, an infrastructure can operate at well below the optimal design state (e.g., because one or more units, subsystems, or systems have failed) and still provide what the user perceives as full service."[14]

At any point in the continuum, the state of operation is a function of interrelated factors and overall system conditions.

Australia's 2023 Critical Infrastructure Resilience Strategy (the Strategy) defines critical infrastructure as: "those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security."[15] The Strategy states that Federal, State and Territory Governments should: "Understand cross-sector dependencies and collectively work to address sectoral vulnerabilities and resilience gaps."[16]

Dependencies appears multiple times across Australian critical infrastructure policy and legislation, however there is no publicly available guide to terminology.[17]

Figure 3: Utility and network interdependencies



Source: The United States' National Association of Regulatory Utility Commissioners (2005)

Figure 4 outlines the dimensions for describing infrastructure dependencies and provides a frame for further stages of this project.

Dependency is a linkage or connection, and interdependency is a bi-directional relationship between two infrastructures. Interdependency can be further clarified according to physical, cyber, geographic or logical interdependencies (see also Definitional Table in Annex A).

Within other academic literature on critical infrastructure resilience, six primary inter-related characteristics have been identified: management and organizational; safety, social, sustainability, technical, and financial. These are partially represented in Figure 4 as organisational and operational characteristics' and further extrapolated in Table 4 in Annex B.[18]

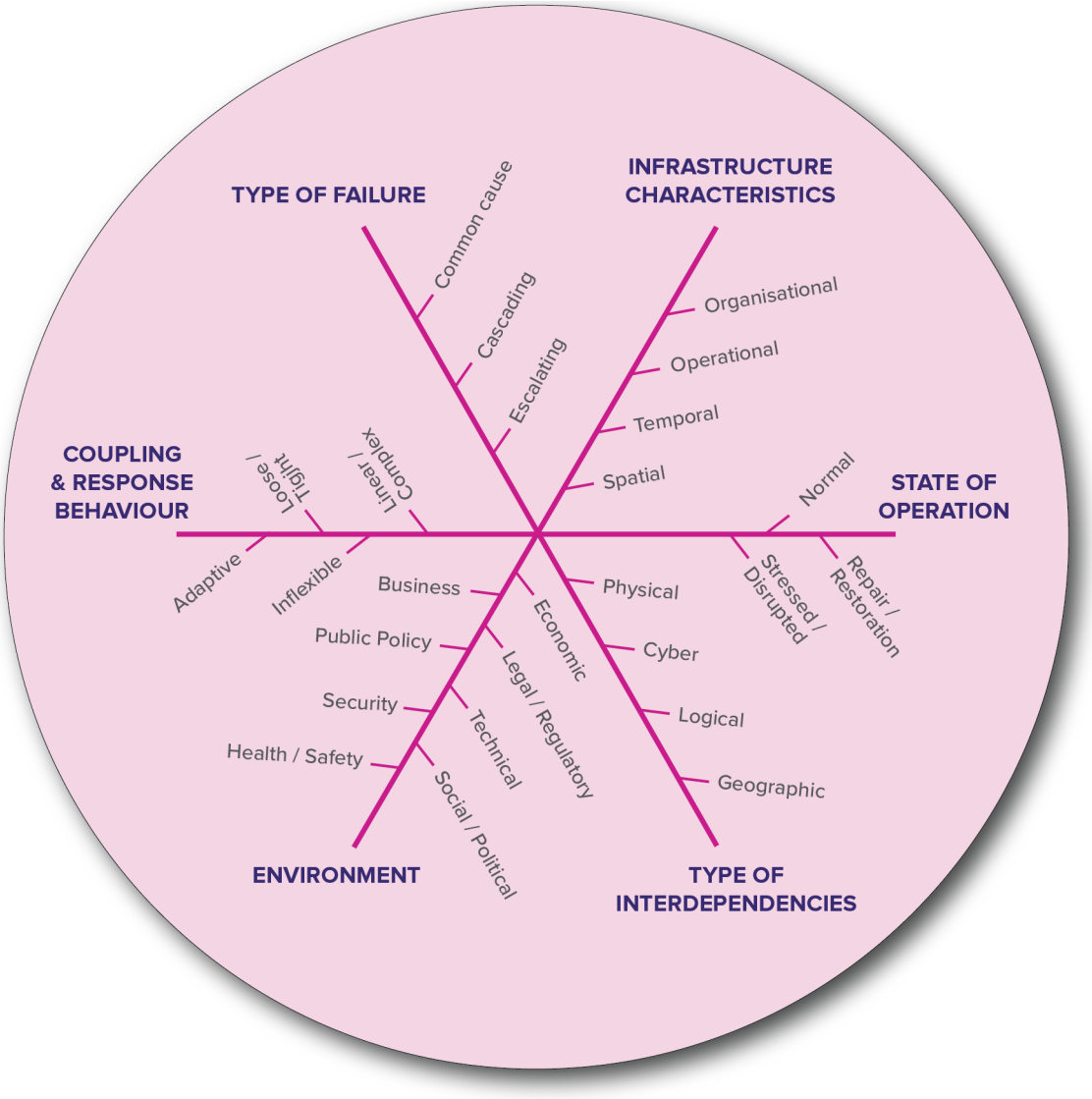
The spatial dimensions refer to the pertinent scales of infrastructure ranging from part, unit, subsystem, system, infrastructure, and interdependent infrastructure. The temporal range of infrastructure assets can range from milliseconds in the instance of data communications to years in the case of infrastructure planning.

In short, there has been a tendency to think about and plan for resilience at the enterprise level, however, at the sector level, the problem space is different.

Resilience-based approaches inherently review how the structure and activities of systems influence one another and serves as an avenue to understand and even quantify a web of complex interdependent networks and their potential for disruption via cascading and escalating systemic threat or types of failure.[19]

At the sector level, resilience involves looking for cross-network and other collaborative opportunities for response behaviour, identified in Figure 4 as adaptive, linear, loose/tight and inflexible, and referred to in resilience literature as absorptive, adaptive and transformative capacities of critical infrastructure systems (see Annexes B and C).

Figure 4: Dimensions for describing infrastructure interdependencies



Source: Rinaldi et al. (2001)

4. Resilience of what system: defining the telecommunications sector

Working definition of the telecommunication sector

The purpose of the telecommunications sector is to enable communication to intended recipient through the transmission, reception and/or delivery of information or data (the Purpose).

The services provided by the telecommunications sector include network, data, voice, mobile, cloud, and wireless services (Services).

The assets that enable these services include physical infrastructure, data centres, networks, and operational port systems (Assets).

The sector is made up of those that provide these Services and/or Assets for the Purpose, their supply chains, as well as consumers and regulators.

Defining the technology to produce a 'sector profile' is difficult given the large number and variety of organisational entities, infrastructural assets, regulatory definitions, and emerging technologies.

A working definition has been developed building on the Australian Bureau of Statistics definition of the communications sector.

This project takes an expansive definition that considers the convergence of telecommunications with internet, software (including software-defined networks), and cloud infrastructure.

Background

Conventionally, there has been a distinction drawn between the *communications* and *telecommunications* sectors. This distinction relies on the view that carriers and carriage service providers are the primary suppliers of fixed broadband, fixed line voice, and wireless services.[20]

For example, the Australian Bureau of Statistics defines the communications sector broadly as comprising the following activities (and their industries):

- Telecommunications services (both fixed and wireless), along with the underlying infrastructure required to deliver these services.
- Terrestrial broadcasting, including free to air television and radio, along with pay TV.
- Australian content production and distribution, including film, television and print media.
- Internet publishing, broadcasting and web search, including over-the-top (OTT) services.
- Postal and courier services.[21]

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts views the *telecommunications* industry as consisting of fixed-line network operators, fixed-line retail or internet service providers, and mobile operators and resellers.[22]

A number of firms provide services across these technologies. Further, for the purposes of the *Telecommunications Act 1997* (Cth), *telecommunications* denotes the carriage of communications by way of guided and/or unguided electromagnetic energy.[23]

Data processing, cloud storage and the internet are increasingly integral to the infrastructure and economics of traditional telecommunications (see Figure 5). Amendments to the Security of Critical Infrastructure Act (2018) (SOCI Act) added the 'data storage and processing sector' as a critical infrastructure sector in its own right.[24]

The working definition above allows that the assets that enable services include both physical infrastructure and virtual assets such as software-defined networks and the operational support systems that keep networks running.

Adding data storage and processing to the definition of telecommunications may collapse the separation between critical infrastructure sectors which are distinct sectors and asset classes in legislation such as the SOCI Act.

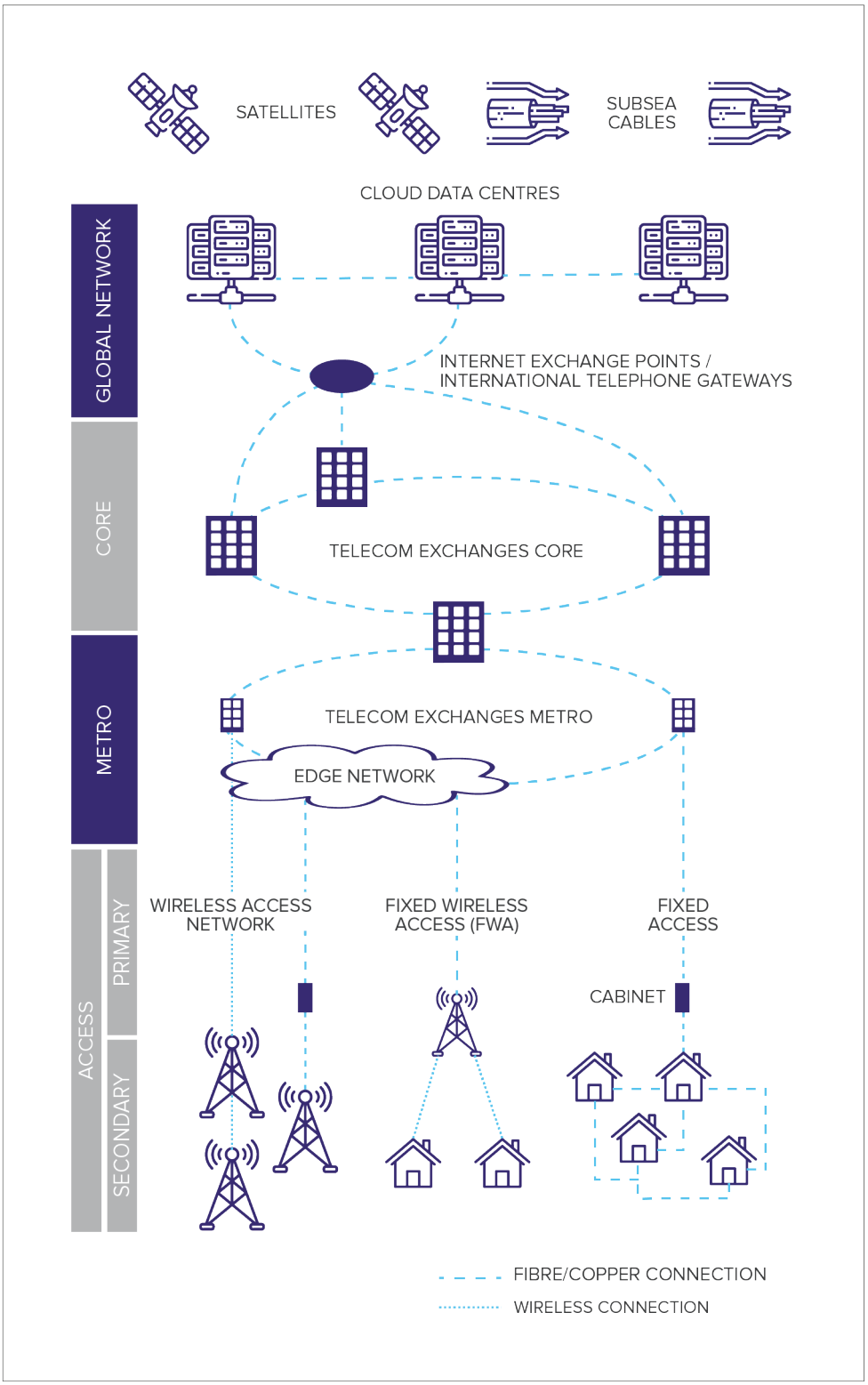
Although the project takes a wide definition of the sector it treats data storage and processing as a critical dependency (see PESTLE).

Figure 5 is a simplified map of the infrastructures and network relationships of the telecommunications sector, adapted from Gotti and Chiarella to include satellites and subsea cables. It does not show providers.

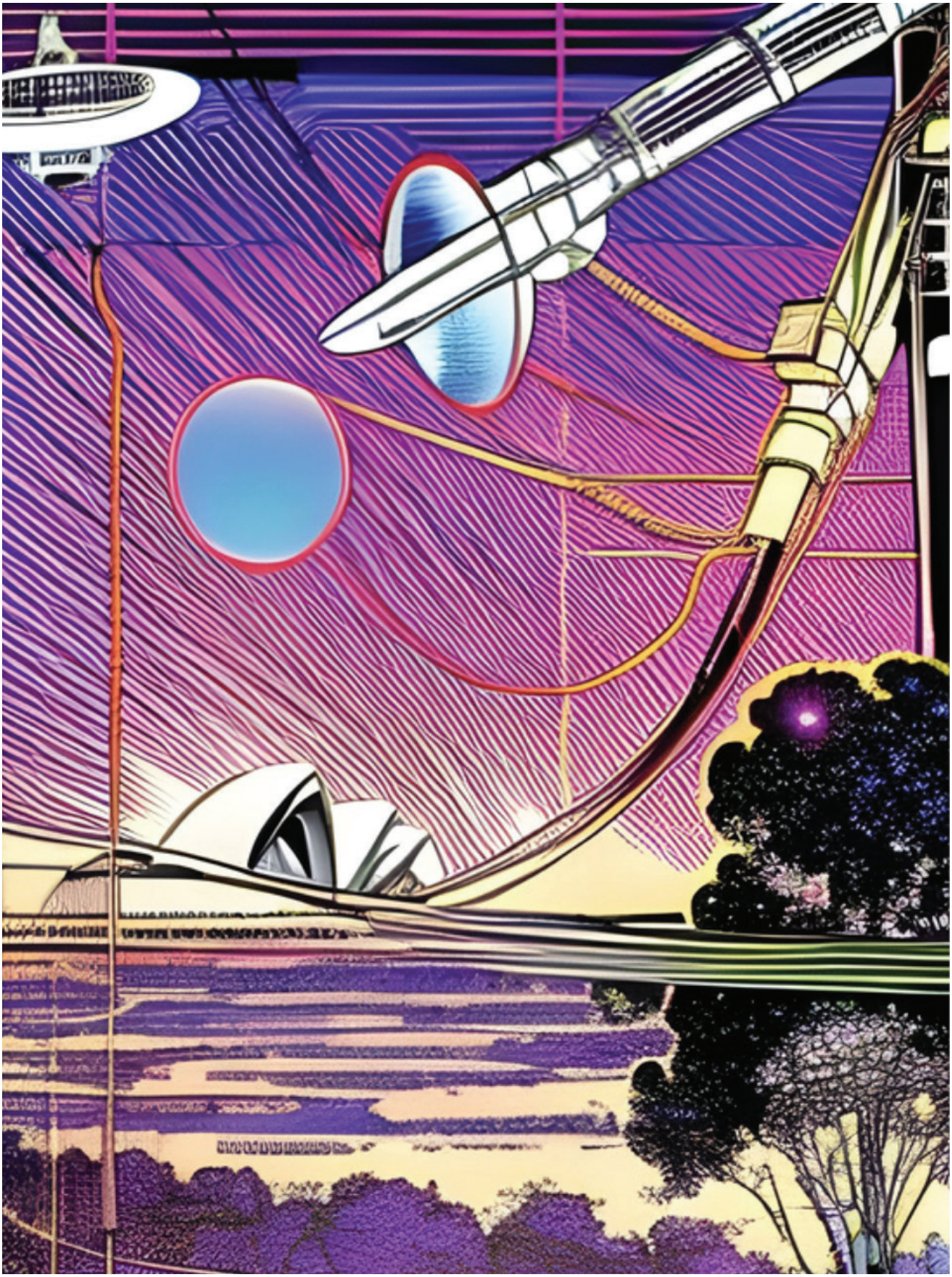
Feedback to the research team by the panel of experts indicated that the traditional view is narrow and does not adequately reflect the nature of telecommunications in an increasingly digitised world.

In accordance with the project's definition of the telecommunication's sector, to be included in the sector, a provider, service, or asset must be for the purpose of enabling communication through the transmission, reception and/or delivery of information or data.

Figure 5: Simplified map of telecommunications network



Source: adapted from Gatti and Chiarella, (2020)



Source: AI generated image via Canva

5. Resilience of who: resilience for owners, operators, government and community

The telecommunication sector is complex and has a high propensity for innovation. This project takes a broad view of *who* this risk and resilience profile may benefit. This includes entities who are 'non-traditional' and do not currently fall under the remit of telecommunications legislation but fall within the working definition of the telecommunications sector as set out in section 4.

These entities and groups are outlined in *Table 1.* Categorical distinctions (i.e., between software providers and equipment manufacturers) are not as clear as the table may imply.

Table 1: Summary of telecommunications entities, functions and examples

ENTITY TYPE	FUNCTION	EXAMPLE/S
Telecommunications carriers	Own and operate the infrastructure and networks used to transmit information	Telstra, Optus, Vodafone and TPG Telecom, Symbio, and Macquarie Telecom
Internet service providers (ISPs)	Provide access to the internet through telecommunications networks	iiNet, Aussie Broadband and Dodo Services, AARNET
Wireless services providers	Provide wireless communication services through cellular networks	Telstra and Optus
Cable and satellite television providers	Transmits television programming through telecommunications networks	Foxtel
Broadcaster	Transmits audio or visual content to a wide audience via radio, television or digital platforms	Australian Broadcasting Corporation (ABC)
Equipment manufacturers	Produce the hardware and software used to transmit and receive information over telecommunications networks	Nokia, Ericsson and Huawei
Software providers	Develop applications and software used to transmit and manage information over telecommunications networks	Microsoft and Cisco
Telecommunications infrastructure providers	Develop, construct, invest in, own and/or maintain telecommunications infrastructure assets	BAI Communications, Field Solutions Group, and Waveconn

System integrator	Design, install and maintain telecommunications infrastructure and systems for businesses and other organisations	Fujitsu, IBM Australia and Accenture
Cloud service providers	Offer cloud computing services to businesses and consumers	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Vault, and Macquarie Cloud Services
Cyber security companies	Provide security solutions for telecommunications networks and systems	CyberCX, Macquarie Government, and SentinelOne
Wholesale network operators	Provide access to their networks and infrastructure to other service providers	National Broadband Network (NBN), Vocus Communications
Data centres and colocation providers	Provide facilities for hosting telecommunications equipment and infrastructure	Equinix, NextDC, and Macquarie Data Centres
Private networks	Private telecom networks, owned by enterprises, universities, or institutions, use 5G/LTE and virtualised infrastructure to create secure, dedicated networks with unified connectivity, low latency, and high capacity within a specific area.	Ericsson, Vodafone and Nokia
Regulatory bodies	Oversee and regulate the telecommunications sector to ensure fair competition, protect consumer interests and promote public interest	Australian Communications and Media Authority (ACMA)
Australian Government	Develops policy, regulates and oversees the industry to ensure that it operates in a fair and competitive manner, and promotes the development of telecommunications infrastructure and services for the benefit of consumers and businesses	Department of Infrastructure, Transport, Regional Development, Communications and the Arts; and Department of Home Affairs
State and territory governments	Manage the licences and permits for the information media and telecommunications industry. Also are responsible for emergency management	
Local councils	Play an important role in network facilities	
Australian public	Consume and use telecommunications products	

6. Resilience to sources of risk: taking an all-hazards approach

This project takes an all-hazards approach to risk management for the telecommunications sector. It will identify, assess, and prioritise potential risk exposures and hazards that the sector faces.

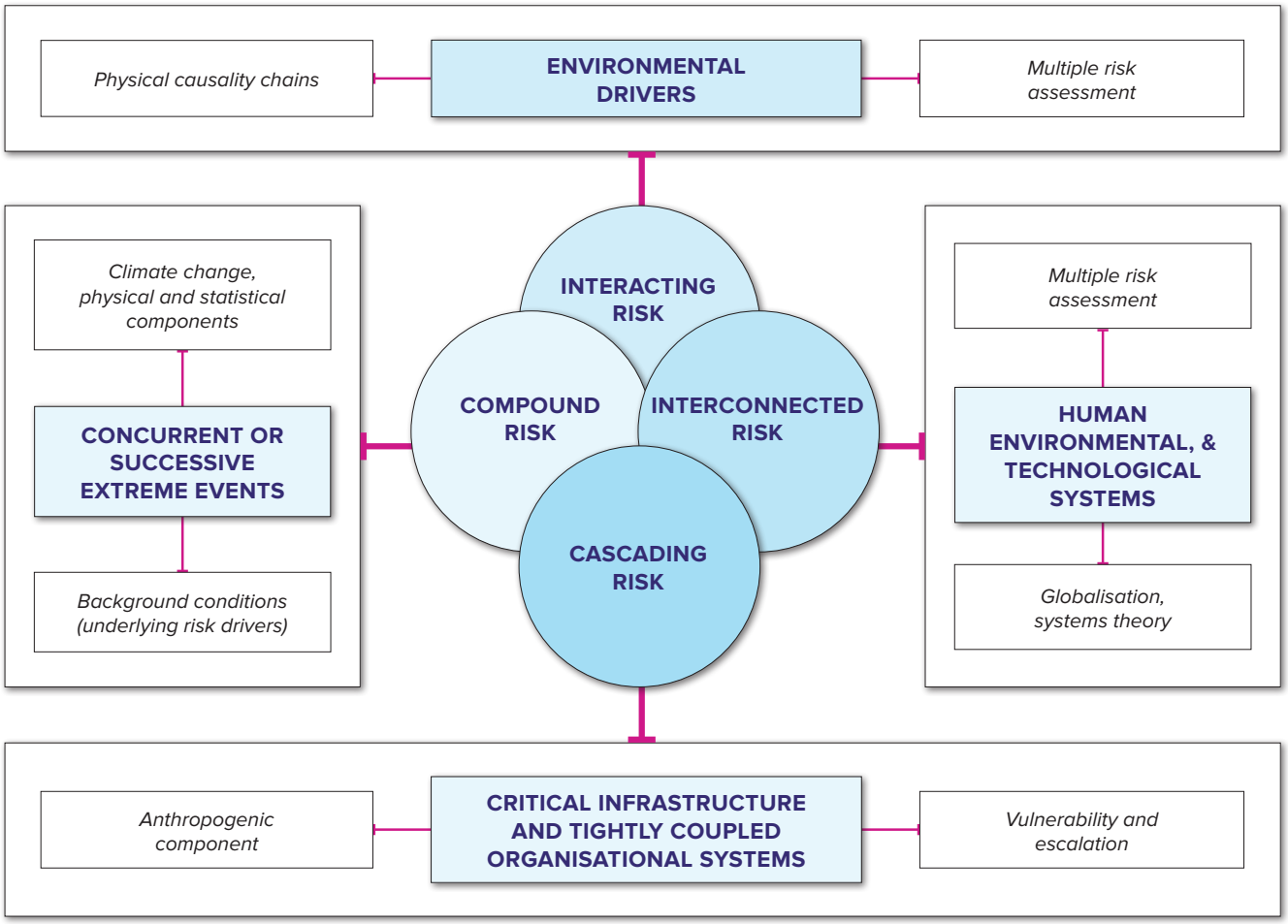
The concept of an all-hazards approach recognises that emergencies and disasters can arise from diverse sources, including natural disasters like hurricanes, earthquakes, floods, and wildfires, as well as human-made incidents such as terrorist and cyber threats, industrial accidents, pandemics, and technological failures. By taking an all-hazards approach, management efforts are not narrowly focused on specific types of events but are designed to be adaptable and flexible to handle a broad spectrum of emergencies.

An all-hazards approach considers the dynamic that can occur when risk compounds, cascades, interacts, and be interconnects (see Figure 6). That is, the approach is meant to be adaptable to the scale and unpredictable interactions that can occur within and between human, technological and environmental systems.

Exploring dynamics of interdependency and risk amplification will deepen our understanding the systemic complexity within the telecommunications sector.

Moreover, it will lead to a holistic view of the sector's vulnerabilities, better enabling key stakeholders to take the necessary actions to protect their critical infrastructure assets and provide essential service continuity for Australians.

Figure 6: A framework for compounding, interacting, interconnected, and cascading risks



Source: Pescaroli and Alexander, (2018)

7. Resilience over what timeframe: dealing with present disruptions and providing a more resilient future

The project considers short and long-term disruptions, the project aims to account for both the legacies and rapid change existing within the sector.

Telecommunications infrastructure dynamics span vast temporal scales from milliseconds (e.g., power system operation) to hours (e.g., emergency response) to years (e.g., infrastructure upgrades).[25]

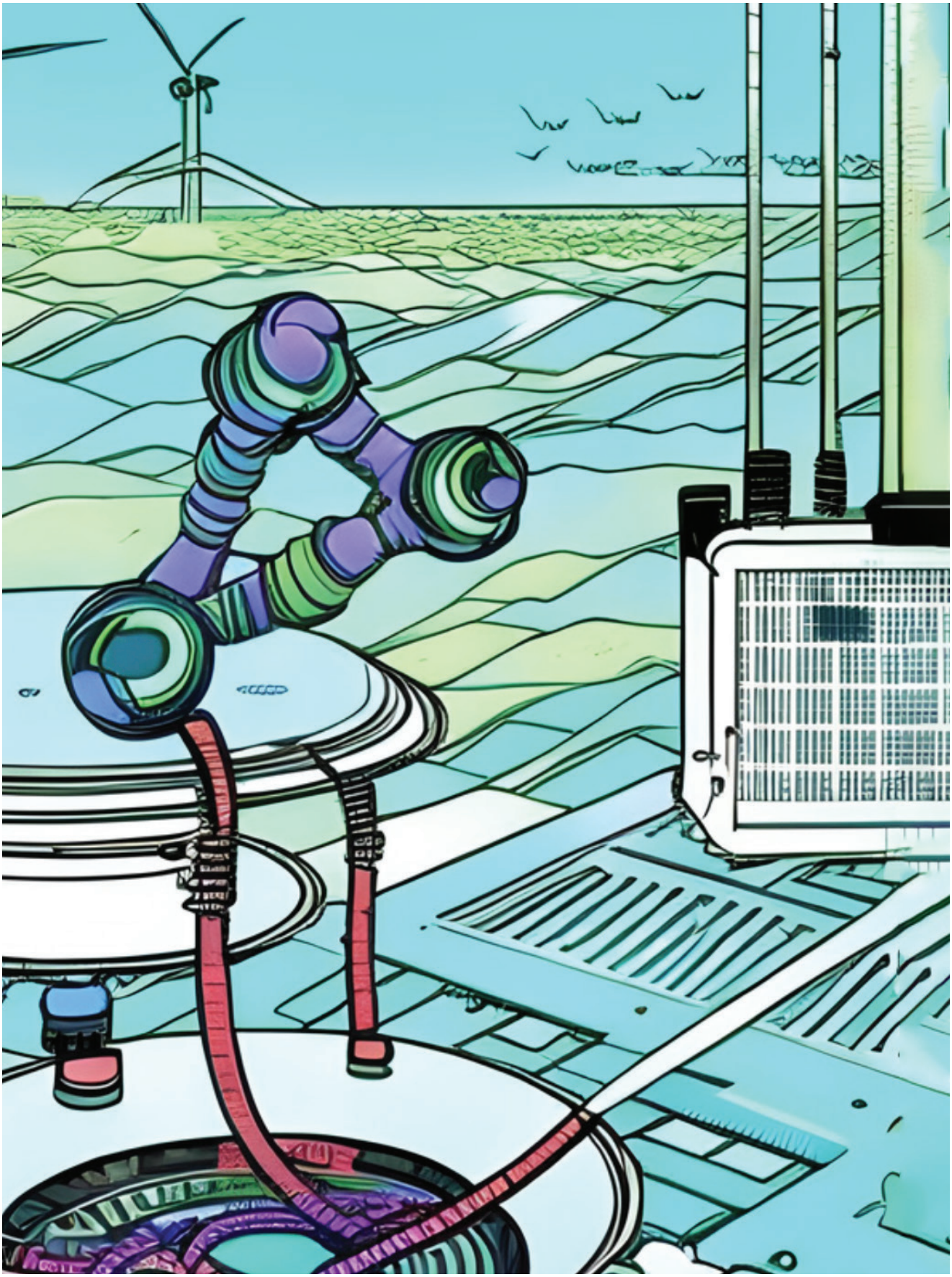
Communications networks are crucial for the livelihoods of Australians and the nation's prosperity – underpinning every sector in the economy.

Failure across communication networks can have serious consequences, affecting the delivery of critical services to Australians, potentially jeopardising public safety and wellbeing, the economy, and national security.

This highlights the importance of anticipating and mitigating potential disruptions and losses within the Australian telecommunications sector over a range of time horizons. The specific periods of time (i.e. over the next two, five, ten, twenty years etc.) will be explored as a component of foresight exercises planned in subsequent stages.

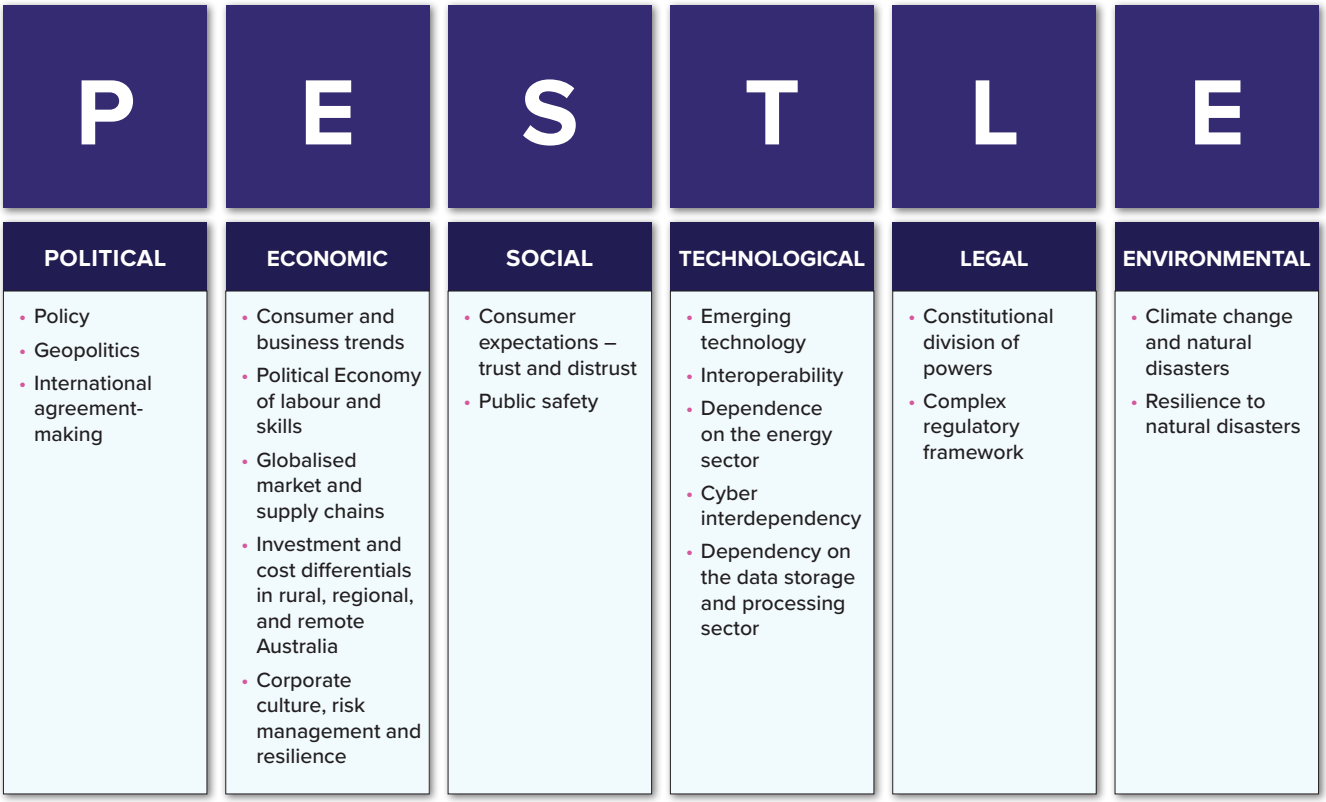
For example, current trends show the growing significance and interdependence of systems that combine physical infrastructure, such as fiber-optic cables, sub-sea cables, and satellites, with advanced data storage capabilities, cloud computing and artificial intelligence.

In turn, this project will create an independent evidence base that can contribute to the sector's ability to withstand unexpected shocks and disruptions over time.



Source: AI generated image via Canva

8. PESTLE Analysis



Introduction

This PESTLE analysis provides a macro-picture of the telecommunication's operating environment.

Political, economic, social, technological, legal, and environmental factors shape the goals and objectives of government, the private sector and consumers. These factors exert pressures, create constraints and interdependencies.

This PESTLE analysis defines the context of the project by outlining the current state, future developments and disruptive changes that may have an impact on the risk landscape and overall resilience of the telecommunications sector. By understanding factors internal and external to the sector — acknowledging that there is substantial overlap — these thematic groupings provide a guide to the influences in the sector.

This analysis will directly inform subsequent stages of the project.

Source: AI generated image via Canva

P

Politics

Summary

The Australian telecommunications sector operates within a landscape shaped by domestic and international political and policy dynamics. These dynamics include government investment decisions, state and federal regulation, geopolitical factors, and international agreements that affect the sector's operations and strategic decision making.

Policy shapes how industry and different levels of government operate, puts boundaries on permissible operational states and influences the growth and market structure of telecommunications.

Policy

Over the past 25 years, Australian Governments have pursued policy principles to promote competition, innovation and investment in the telecommunications market. These policies aim to ensure equitable access to affordable communication services, even when infrastructure owners control essential facilities through access regimes.[26]

Policy has focused on technological and competitive neutrality, network reliability, and universal connectivity. Governments have sought to establish clear, simple, and practical principles based on legal and empirical foundations, while employing mechanisms to subsidise costs in areas where service is less affordable, such as rural, regional, and remote locations.[27]

These regulatory principles produce varied outcomes. The current landscape is defined by concentrated ownership of network infrastructure, creating barriers to entry and reliance on regulatory mechanisms for competition.[28] Prices remain high, data caps exist, and consumer complaints, especially in rural, regional and remote areas, continue to rise annually.[29]

The National Broadband Network Co Ltd. (nbn)—a government business enterprise (GBE)—provides a wholesale broadband access. Australia is one of the few countries with a wholesale fixed broadband network established by a GBE. It was established to address inequity. A fundamental policy setting is that the NBN cannot provide retail services. Notwithstanding the equity motivations, mandating wholesale-only networks to foster service-based competition may perpetuate monopolies and distort infrastructure competition. This cements government as the driver of aspects of network strategy, rather than industry or consumers.

In recent years, Australia has seen oversight of telecommunications sector expand to include more robust national security protections (e.g., Australian Government Guidance to 5G networks) and an increased focus on how reliability and maintenance is sustained and regulated.[30]

State and territory regulations introduce an additional level of compliance. Telecommunications carriers are required to comply with planning laws specific to each jurisdiction (with limited exceptions). Carriers must engage with local councils and landowners to secure leases for the installation of telecommunications infrastructure. These factors frequently pose constraints to infrastructure development.[31]

Regulatory settings have long considered monopoly service provision, however the characteristics of this will have to adapt to the activities of over-the-top-providers. The increasing demand for the development of sovereign capability, driven by national security concerns, is changing dimensions of the design of regulatory solutions.

Geopolitics

The Australian telecommunications sector is dependent on trade with other countries, particularly to import equipment and technologies. Geopolitical factors or changes in trade policies can disrupt supply chains and lead to higher costs.

The sector attracts substantial investment from foreign entities such as the United States, the United Kingdom, and Singapore.[32] Two-thirds of all investment in technology start-ups in Australia involved international capital in 2021.[33] Geopolitical tensions or changes in foreign investment policies can impact the level of investment in the sector.

The country's history as a technology adopter means a high level of dependence on global technology providers.[34]

There have been concerns about the involvement of foreign companies that may be subject to extra judicial direction by a foreign government in the development of 5G technology.[35]

The current geopolitical environment is increasing the risk of fragmentation and divergence in global technical infrastructure, such as the internet.[36] Concurrently, however, there are instances of convergence and harmonisation, such as the EU Digital Single Market.[37]

Companies have had to adapt to this heightened geopolitical environment, diversifying their supply and sourcing strategy to ensure that it is not dependent on one facility, one manufacturer, or one location.

International agreement-making

To respond to the growing threats in an increasingly connected world, countries are strengthening their focus on network security and associated requirements, addressing the security of supply chains, and streamlining reporting and information-sharing processes. Governments are increasing scrutiny and oversight of industry and imposing stricter enforcement measures.

International fora, such as the International Telecommunications Union (ITU), the Internet Engineering Taskforce (IETF), the Internet Assigned Numbers Authority (IANA), the Global System for Mobile Communications Association, and the World Wide Web Consortium (W3C), play crucial roles in shaping and advancing the field of telecommunications and internet technology.

The agreements reached within these fora – including voluntary standards, protocols, and requests for comments (RFCs) – have the potential to significantly influence the interoperability and commercial viability of technologies.

By shaping and defining these agreements through consensus, these international organisations have a direct impact on the development and functioning of telecommunications systems worldwide.

Having multiple, conflicting frameworks can create confusion and complexity.

E

Economic

Summary

The telecommunications sector faces economic challenges related to consumer dependence, labour and skills, global market competition, and rural investment disparities, requiring strategic interventions to bridge the digital divide and promote equitable access to high-quality services for economic growth.

Greater bandwidth has generated more traffic as consumers stream and download greater volumes of content. Telecommunications providers are needing to invest in technology upgrades to maintain and grow their subscriber base but need to generate revenue from these upgrades.

There is growing evidence of the socio-economic impact of telecommunications infrastructure deployment on economic growth, local development, labor market, firm productivity and entrepreneurship.[38] As a result of numerous geopolitical and macroeconomic factors, inflation is forecast to remain high in 2023–2026 timeframe affecting the overall investment environment.[39]

Consumer and business trends

The COVID-19 pandemic accelerated Australia's digital transformation, with remote work and virtual collaboration becoming the new norm.[40] Demand increased for telecommunications services, particularly for video conferencing, cloud-based collaboration tools, and online entertainment platforms.[41]

Businesses are moving their digital assets to the cloud. The growth of e-commerce, advanced analytics and emerging technologies like automation and artificial intelligence is further driving demand for high-speed infrastructure and investment to drive the adoption of 5G.[42] A rising number of businesses and consumers only use digital payments, which are dependent on telecommunications network availability.[43]

The political economy of labour and skills

Near-term predictions put the number of technology workers in Australia to over 1 million by 2024, and 1.2 million by 2027.[44] As reported by the Tech Council of Australia, the nation will need more than one million people in technology-related jobs by 2025.[45]

The COVID-19 pandemic has impacted the influx of overseas technology workers, leading to a greater emphasis on domestic enrollments in IT degrees and the re-skilling of workers from related sectors. Declines of workers are predicted in Telecommunications Trades, which may impact the maintenance of legacy infrastructure.[46]

Australia has skill shortages in, particularly in software, application programming and cyber security.[47] National security concerns and the need for sovereign capability are increasing the demand for onshore skills and changing the security requirements of offshore providers.

The globalised market and supply chains

The COVID-19 pandemic re-opened debate about the costs and benefits of highly coordinated global supply chains in manufacturing. Reliance on single-source suppliers and lack of transparency has led to more attention on diversity and geography of supply chains. A shortage of semi-conductors was one of the most acutely felt areas of disruption.

Despite challenges to supply, many companies were able to adapt and, through their robust supply chain practices, meet heightened demand for telecommunication services.

With global technology companies expanding their footprint in Australia, competition in the market has intensified.[48]

The globalised market has created opportunities for the outsourcing of certain functions within the telecommunications sector. While this brings efficiency and cost savings, it also increases the likelihood that the domestic sector will be impacted by supply chain disruptions and geopolitical uncertainties.

Additionally, as entities – such as those responsible for subsea cables or data – operate across multiple jurisdictions, regulatory compliance and intellectual property protection become more complex.

Open-source software supply chains have recently come within the purview of national security agencies.[49] Maintaining open-source software neutrality (e.g. software as a public good) as a fundamental input of proprietary systems may increasingly be tested by a range of commercial, regulatory and geopolitical factors.

Investment and cost differentials in rural, regional, and remote Australia

Telecommunications investment and cost disparities in rural, regional, and remote Australia hinder access to affordable and high-quality services. The Australian government has implemented initiatives like the Mobile Black Spot Program[50] and the Better Connectivity Plan for Regional and Rural Australia[51] to address these challenges.

Targeted investment in rural and regional areas will continue to be a priority for the telecommunications sector, given its crucial role in enabling participation in the digital economy. For example, the provision of private telecommunications networks, such as 5G, to mining, rail and agricultural enterprises will improve the ability of those sectors to automate and achieve productivity gains.[52]

The Universal Service Obligation (USO) is a consumer protection policy to ensure reasonable access to voice and payphone services. The Government has established a new Universal Service Guarantee (USG) to extend USO to voice *and* broadband services, regardless of location.[53] The extension to broadband reflects the Productivity Commission's recommendation to replace the current contract 'to reflect changing policy, market and technological realities.'. [54]

The 2021 Regional Telecommunications Review highlighted the necessity for improved mobile and broadband services, emphasizing the existing gaps and the importance of infrastructure investment in regional areas.[55]

Corporate culture, risk management and resilience

Effective risk management in the telecommunications sector involves identifying, assessing, and mitigating potential losses from financial, operational, strategic, reputational, and environmental risk exposures. However, it is common for risk management to be reduced to a compliance exercise, lacking proactive exploration, and understanding of potential risks.

In addition to risk management, stakeholders and experts emphasised the importance of resilience – which focuses on an organisation's ability to adapt and recover from unexpected disruptions through continuous monitoring and adjustment. Many observed that the resilience culture is less mature than the risk culture.

How companies intersect with 'national resilience' is a gap in current corporate resilience approaches.

S

Social

Summary

Access to reliable telecommunications services is crucial for all Australians, serving as the foundation for business operations, government services, social interaction, and public safety. However, the current telecommunications landscape highlights challenges in information and network sharing among states and territories, resulting in negative consequences for consumers and emergency management efforts.

Consumer expectations – trust and distrust

Telecommunications in Australia are regarded as a social necessity and consumers are increasingly dependent on services to participate in civic life (including banking, schooling, and access to government services).

Consumers expect telecommunications services to be affordable, reliable, and accessible regardless of location or socioeconomic status. Consumer trust plays a role in determining the uptake of innovative technologies.

In addition to basic connectivity, consumer have increasingly higher demands for high-speed internet, mobile connectivity, streaming video, online gaming, and cloud storage. The increased frequency of natural disasters has changed the expectations of customers toward providers about network coverage, outages or other issues that may affect service delivery.

The telecommunications sector is grappling with an erosion of consumer trust, in part driven by recent cyber incidents, such as the 2022 Optus data breach. According to the Roy Morgan Trust Survey, a majority of Australians either lack trust in any telecommunications provider or distrust all providers in the sector.[56] The 2023 Edelman Trust Barometer reported a similar decline in consumer trust, with the telecommunications industry experiencing one of the largest drops in trust within a one-year timeframe.[57]

Public safety

Successive catastrophic natural disasters (bushfires, floods and cyclones) have intensified the need for advanced public safety communications. Public Safety Agencies (PSAs) today often rely on legacy LMR/PMR (Land Mobile Radio/Private Mobile Radio) networks, together with mobile network operators (MNOs) for their voice and data communications. This has resulted in a significant capability gap between the networks used by PSAs and those used by citizens:

1. Citizens Command & Control centers are unable to share in real time images, video, and other situational awareness information with first responders that could be used to provide safer and more effective first response.
2. First responders are unable to share and analyze images, video, and other situational awareness information among themselves to support safer and more effective first response.

In short, legacy LMR networks are inadequate to meet the challenges of today and the future, which is why PSAs globally are increasingly migrating to public safety mobile broadband (PSMB).

In May 2023, the Australian Government announced $10.1 million to establish a central Taskforce to drive the delivery of a Public Safety Mobile Broadband (PSMB) capability across all of the states and territories.[58]

PSMB capability would deliver a mobile broadband service that provides Public Safety Agencies (PSAs) and first responders with fast and secure voice, video and data communications.

A new cell broadcast National Messaging System (NMS) will use new 'real-time' Cell Broadcast technology to significantly enhance how the Commonwealth delivers emergency messages across the states and territories. The present Location Based Solution using SMS means that emergency messages only go to customers with coverage in the area subject to the alert. Cell Broadcast is a solution that sends an alert to everyone within the radius of the cell site broadcasting the alert, regardless of customer status.

T

Technological

Summary

The Australian telecommunications sector is experiencing a transformative phase with the emergence of new technologies alongside the reshaping of telecommunications infrastructure and network architecture.

The network typology of telecommunications is changing at the global and local levels due to the increased importance of cloud computing, the growth in Internet-of-Things (IoT) and sensors, and the next generation of communications enabled by 5G and 6G.

More connected devices transmitting more data is creating higher peaks of network utilisation. Upgrading or expanding existing infrastructure to accommodate escalating data demands is complex and costly. There are mounting competitive pressures from over-the-top providers targeting cornerstones of telecom business.

Cross-carrier roaming, or network interoperability, is an area of contention between government and industry. The ACCC is conducting an inquiry into the technical feasibility of mobile roaming and tower usage especially in times of natural disaster.[59] This is an area of development in the immediate future.

The sector has a critical dependency on the power-grid. The functioning of telecommunications is central to the day-to-day activities of other critical infrastructures.

Emerging technologies

Technological advancements have ushered in new configurations of telecommunications services.

Cloud computing, referring to the delivery of data storage, processing and applications over the internet is transforming the telecommunications sector.

5G wireless networks offer fast connectivity that allows IoT devices to communicate and share data.

Edge computing, referring to the processing and analysing data closer to the source of its generation, holds advantages in scenarios where real-time, or near-real-time processing is necessary.

The Internet of Things (IoT) has emerged across a range of use-cases including smart-grids, industrial automation and in emergency services. IoT represents numerous opportunities for businesses to collect and analyse data, improve operational efficiency, and increase a range of outcomes including increasing economic productivity.

Artificial intelligence (AI) enabled technologies that use machine learning and natural language processing have already found their place in telecommunications, enhancing network management, data analysis, customer service, and cyber security.

Carriers are investigating the use of both Low Earth Orbit (LEO) satellites and Medium Earth Orbit (MEO) satellites in network models. Their deployment of Low Earth Orbit (LEO) satellites can increase capacity, reduce latency, and widen coverage for voice, messaging and certain data uses (i.e.d IoT devices). LEO satellites have the potential to provide high-speed internet access to remote and underserved areas

with limited terrestrial infrastructure. They can also serve as backup communication systems for remote cell sites during emergencies, facilitating quick and efficient communication between impacted areas and first responders.

Interoperability

Cross-carrier roaming, or network interoperability, could allow customers to use another carrier's network outside their coverage area without excessive fees.

It could play a crucial role in maintaining telecommunications services during and after disasters by enabling access to alternative networks when infrastructure is damaged. This benefits emergency services, first responders, and affected communities, but requires coordination, infrastructure investment, and regulatory collaboration among carriers.

Economic, technical and regulatory barriers, as well as commercial willingness, have hindered its implementation in Australia. The ACCC is conducting an inquiry into the technical feasibility of mobile roaming and tower usage, with a report due by 30 June 2023.[60]

Dependence on the energy sector

Australia's telecommunications sector is dependent on the energy sector to power its network infrastructure, including mobile towers and data centers.

A review by the Australian Communications and Media Authority revealed that 88% of telecommunication outages during the 2019-2020 bushfires were caused by mains power outages.[61]

Power-grid infrastructure is a critical area of dependence as disruptions from natural disasters or energy supply issues – such as by grid overload, human error, interference, or equipment failure – can lead to service loss.

The Royal Commission into National Natural Disaster Arrangements emphasised the importance of coordination between the energy and telecommunications sectors to ensure operational continuity during emergencies. Establishing protocols for collaboration was recommended.[62]

Cyber interdependency

Pervasive computerisation is intensifying system interconnectedness and hence cyber interdependencies which can heighten impacts of service disruptions and cyber security threats.

The increase move to the cloud also amplifies concerns about cyber threats and potential disruptions due to downtime or service interruptions.

The emergence of new technologies broadens the attack surface for cyber threats down to the device level, while advancements in innovative technologies enable attacks to propagate at an accelerated pace.

All emerging technologies have vulnerabilities. Vulnerabilities are the conditions determined by physical, social, economic, and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards.[63] In common international standards, vulnerabilities are classified according to asset class to which they relate: hardware, software, network, personnel, physical and organisational factors.[64]

Cyber security cuts across all these factors. Despite best intentions and adherence to international or industry standards, vulnerabilities in design, material, auditing, cryptographic protocols, training of personnel, area of deployment, or power source, can all be sources of eventual damage or disruption.

To address these issues, the telecommunications sector has invested in redundancy measures, cyber security enhancements, and contingency plans to ensure uninterrupted connectivity and safeguard against potential disruptions.[65]

The timescale for the development of a large, fault-tolerant Quantum Computer capable of running analytic algorithms that threaten modern day cryptography is uncertain. However, it is considered by the GSM Association that there is there is a significant (>30%) likelihood that such a computer will emerge by 2032. This likelihood requires preparation, particularly because some forms of cyber threats may be retrospective.[66]

Dependence on the data storage and processing sector

Data processing and cloud storage are increasingly integral to the infrastructure and economics of traditional telecommunications.

The regulation of critical infrastructure under the Security of Critical Infrastructure Act 2018 (the SOCI Act) places obligations on specific entities in the electricity, communications, data storage or processing, financial services and markets, water, health care and medical, higher education and research, food and grocery, transport, space technology, and defence industry.

SOCI amendments added the 'data storage and processing sector' as a critical infrastructure sector in its own right.[67]

L

Legal

Summary

The Australian regulatory environment is complex and characterised by multiple regulatory bodies with overlapping jurisdictions. This often results in conflicting regulations and compliance requirements between state, federal and territory levels of government.

Moreover, the legislative framework is facing challenges in keeping pace with the rapid advancements in technology, complicating the overall regulatory framework.

A challenge is not only enacting new legislation, but also demonstrating readiness to repeal outdated laws instead of continually amending them.

The constitutional division of powers between the Commonwealth and states/territories creates tensions, including to reporting, network connectivity and emergency response times.

Constitutional division of powers

Australia's constitutional democracy divides powers between the Commonwealth and the states/territories.

The Constitution grants the Australian Government responsibility for telecommunications; states/territories are responsible for emergency management. This division creates conflicts particularly in periods where emergencies are increasing in frequency and severity.[68]

The Australian Government Crisis Management Framework (AGCMF)[69] establishes the government's leadership in nationally significant emergencies, covering various crises such as cyber and terrorist incidents, natural disasters, and health pandemics.

However, the AGCMF primarily focuses on immediate response and early recovery, not on pre-planning and transformation. While intending to foster cooperation, it creates conflicts due to the constitutional powers of states/territories to manage crises independently.

Furthermore, deficiencies persist in nationally coordinated approaches to information sharing, asset monitoring, and resource deployment in crisis situations.

Complex regulatory framework

The telecommunications sector is subject to a range of regulations and compliance requirements that can be a challenge for corporate entities to navigate. Industry is obligated to report to a number of regulators across multiple jurisdictions (see Table 2).

The regulatory landscape affects the ability of government to monitor a range of technological issues, including network outages.

A key concern expressed by industry stakeholders in Stage One included complexity and fragmentation resulting in confusion and compliance difficulties for corporate entities.

A range of regulations, including the *SOCI Act*, were identified by stakeholders as overly prescriptive and not fully accounting for the complexity of the critical infrastructure asset classes on which it bears.

Further, stakeholders felt that the inability of some key departments at the federal level to explain the implications and reporting requirements of their own policies and the lack of feedback mechanism creates an environment that is, at times, not conducive to cooperation between industry and government.

High compliance costs and lengthy approval processes were seen to create barriers to entry, particularly for smaller enterprises.

Regulators were seen by industry to be slow to adapt to technological advancements and market changes, lacking the agility needed in a rapidly evolving sector.

While regulation is acknowledged as important, stakeholders emphasise the need for greater industry consultation and co-designing policy changes in the future.

Table 2: Australian regulators, role and responsibility

ACTOR	GENERAL ROLE	KEY INSTRUMENTS
Australian Communications and Media Authority (ACMA)	Government entity regulating broadcasting, radio-communications, telecommunications and online content.	• *Australian Communications and Media Authority Act 2005 (Cth)* • *Broadcasting Services Act 1992 (Cth)* • *Do Not Call Register Act 2006 (Cth)* • *Radiocommunications Act 1992 (Cth)* • *Spam Act 2003 (Cth)*
Australian Competition and Consumer Commission (ACCC)	Government entity enforcing the *Competition and Consumer Act 2010* and other legislation to promote competition, fair trading and regulations of national infrastructure, including telecommunication specific elements of the Competition and Consumer 2010 Act.	• *Competition and Consumer Act 2010*
Attorney-General's Department/ Communications Access Coordinator	Government agency working to maintain and improve Australia's law and justice framework. Through the Australian Government Solicitor, they provide legal services to the Commonwealth.	• *Copyright Act 1968 (Cth)* • *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* • *Telecommunications (Interception and Access) Act 1979 (Cth)*
Department of Infrastructure, Transport, Regional Development and Communications	Government department providing policy direction for the telecommunications sector.	• *Australian Communications and Media Authority Act 2005 (Cth)* • *Enhancing Online Safety Act 2015 (Cth)* • *National Broadband Network Companies Act 2011 (Cth)* • *Telecommunications Act 1997 (Cth)* • *Telecommunications (Consumer Protection and Service Standards) Act 1999* • *Telecommunications (Industry Levy) Act 2012 (Cth)*
State and Territory Governments	Each state and territory maintains emergency management and natural disasters plans at a jurisdictional, regional and local level, and systems for developing, reviewing and implementing those plans.	• A range of emergency management legislation
Local Governments	Each local government plays a central role in the planning and approval process for new telecommunications sites, as well as the removal and remediation of sites that are no longer required.	• A range of local planning laws
Department of Home Affairs/ Cyber and Critical Infrastructure Security Centre	Government department administering national security, cyber security, and telecommunications infrastructure resilience regulations, including data retention obligations and interception rules	• *Telecommunications (Interception and Access) Act 1979 (Cth)* • *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* • *Security of Critical Infrastructure Act 2018 (Cth)* • *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)*
Telecommunications Industry Ombudsman (TIO)	Government entity funded by industry providing independent dispute resolution for consumers and small businesses. Handles complaints about telephone, internet and other services.	• *Telecommunications (Consumer Protection and Service Standards) Act 1999*

Communications Alliance	Private, industry funded entity representing the overall interest of the Australian communications industry. It works together with industry to develop industry Codes which can apply to those who agree to be bound, or if the Code is registered by the regulatory authority, it can bind the whole industry.	• Various industry codes, standards and guidelines.
Communications Compliance	Private entity funded by industry monitoring compliance with Telecommunications Consumer Protection (TCP) Code through annual attestations of compliance with the Code by industry participants	Telecommunications Consumer Protection (TCP) Code

E

Environmental

Summary

Australia's changing climate is creating significant challenges for the telecommunications sector due to heightened average temperatures, shifts in rainfall patterns and a sharp increase in the frequency and severity of natural disasters.[70]

Climate change and natural disasters

In the last five years, the nation has been impacted by a series of catastrophic weather events. Bushfires, floods, storms, and cyclones are anticipated to occur with greater frequency in the coming years as the effects of climactic change worsen.

The likelihood and recurrence interval of natural hazards will change under future projected climate change scenarios.[71] There is a high potential for different climate variables dependent on whether global warming exceeds temperatures of 1.5°C, 2.0°C, or 3.0°C above pre-industrial levels[72], thus creating previously unanticipated hazards.

The telecommunications sector will be tested in its preparation for anticipated hazards. Floods, fires, and storm-damage will threaten infrastructural integrity and service continuity, reduced service due to extreme heat related power outages.

Subsea cables, which enable more than 95% of global digital data transfer, are expected to experience greater vulnerability to climactic-related events such as off-shore storm surges, earthquakes, and submarine landslides.[73]

Adverse weather, including solar flares, cloud cover or heavy precipitation can also affect telecommunications operations.

Although recent natural disasters have shown that the providers of telecommunications services and infrastructure, as well as governments, can be adaptable in unprecedented times of emergency, they too have revealed where real vulnerabilities exist in the resilience of the sector.

Resilience to natural disasters

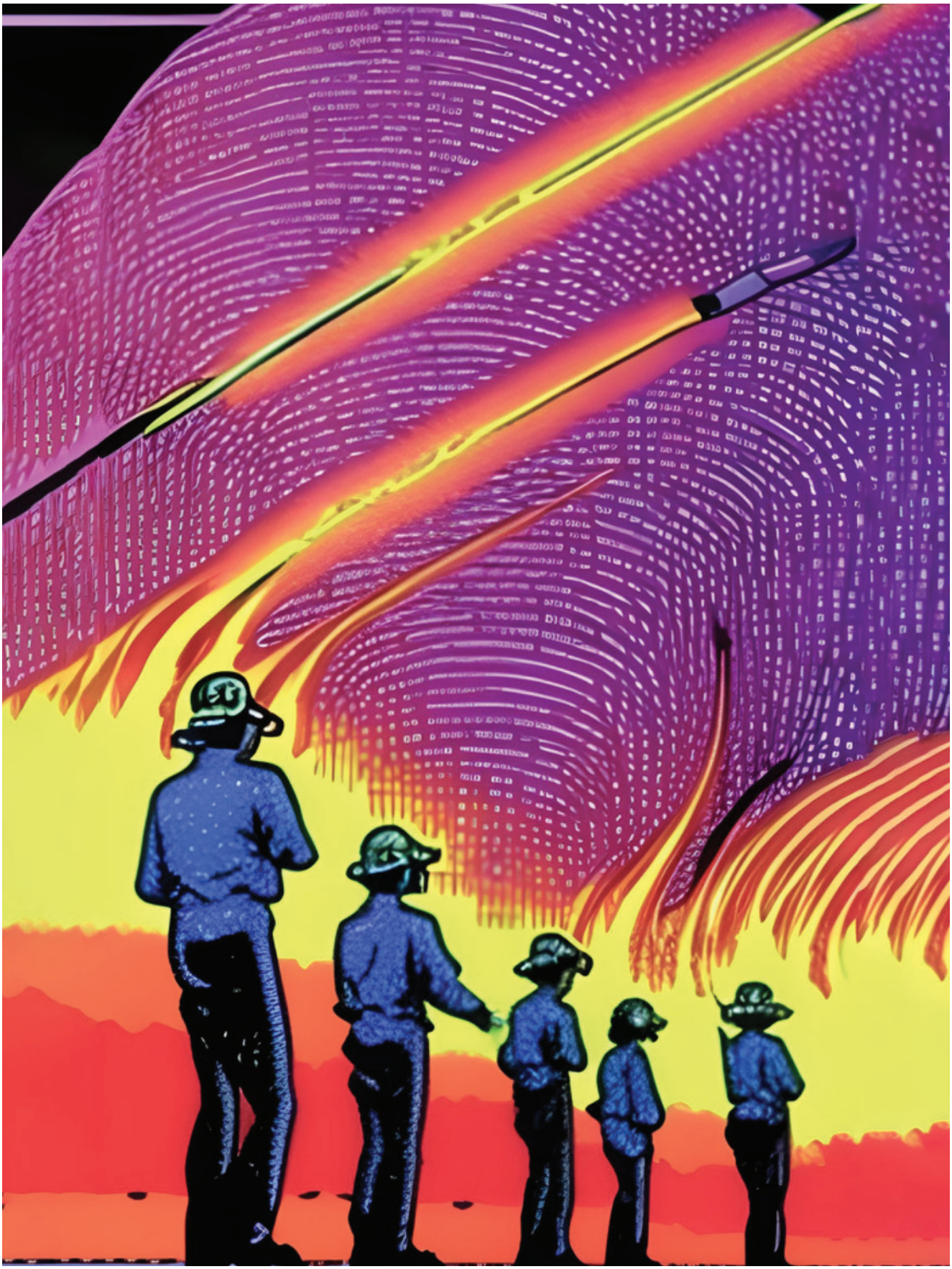
The Australian Government has committed $10.1 million to establish a Taskforce to drive the delivery of a Public Safety Mobile Broadband (PSMB) capability, led by the National Emergency Management Agency (NEMA).[74]

A national PSMB capability will provide emergency services personnel with fast, safe, and secure voice, video and data communications and instant access to critical information in emergencies. The PSMB will enable real time data analytics, situational awareness, and cross-border communications—for example, between ground crews, aerial assets, and incident control centres.[75]

Australia has had a plethora of inquiries into natural disasters, such as the recent Royal Commission into National Natural Disaster Arrangements (2020) and the NSW Bushfire Inquiry (2020). It is unclear whether post-disaster inquiries "produce useful learning" or have recommendations implemented systematically.[76]

Information-sharing at the sector level – between utility providers and telecommunications service providers, or between other key players in the industry – and with government is far from systematic. In instances where recommendations are made, there is no guarantee that implementation will occur, partially because feasibility and cost are not considered to their full extent.

In addition to implementing preventive resilience measures, stakeholders expressed uncertainty regarding whether sufficient reviews of emergencies and information-sharing of lessons learned occurs between industry and governments.



Source: AI generated image via Canva

1 Annex

A. Working Definitions

Table 3: Table of terminology

All-hazards	Accounting for all forms of human, technical and natural threats, ranging from terrorism and sabotage to technical system failures and natural disasters.[77]
Cascading risk	Cascading events can be viewed as the manifestation of vulnerabilities accumulated at different scales, including socio-technological drivers.[78]
Compound risk	Refers to the environmental domain, or to the concurrence of natural events. Eventually, it can be correlated with different patterns of extreme impacts caused by climate change. Institutional definitions tend to focus more narrowly on the hazard component of disaster risk.[79]
Disruptions and disturbances	An event that prevents, or interrupts, the usual functioning of a telecommunications system or network.
Dependency	A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.[80]
Event	Occurrence or change of a particular set of circumstances[81] • An event can be one or more occurrences and can have several causes. • An event can consist of something not happening. • An event can sometimes be referred to as an “incident” or “accident”.
Exposure	The inventory of elements in an area in which hazard events may occur. While literature and common usage often mistakenly conflate exposure and vulnerability, they are distinct. Exposure is a necessary, but not sufficient, determinant of risk. It is possible to be exposed but not vulnerable. However, to be vulnerable to an extreme event, it is necessary to also be exposed.[82]
Hazard	The possible, future occurrence of natural or human-induced physical events that may have adverse effects on vulnerable and exposed elements.[83]

Interacting risk	Refers to the domain of physical relations developed in the natural environment and to its casual chains. They focus on the area in which hazard interacts with vulnerability to create disaster risk. The study of interacting risk be the focus of disciplines such as geophysics and physical geography, while giving space to multiple risk assessment tools and strategies. For example, the study of the dynamics of interacting risk can be translated into simulations and models for the energy industry, thus defining better hazard maps.[84]
Interconnected risk	Used more often in network science and in studies of global interlinkages. It can include the complex interactions between human, environment, and technological systems, which can be translated, for example, into coherent multiple risk assessments or network analysis. Interconnected risk may be referred to as the physical interdependencies that allows societal interactions, and thus a precondition for cascading risk.[85]
Interdependency	A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.[86] • Two infrastructures are **physically interdependent** if the state of each is dependent on the material output(s) of the other. • An infrastructure has a **cyber interdependency** if its state depends on information transmitted through the information infrastructure. • Infrastructures are **geographically interdependent** if a local environmental event can create state changes in all of them. • Two infrastructures are **logically interdependent** if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.
Resilience	Resilience in the telecommunication sector is the capacity to anticipate, absorb, recover, adapt and transform from disruptive events by identifying, understanding, and analysing interdependencies to clarify types of failure, and necessary response behaviour. This may involve boosting infrastructure characteristics (management and organisational, safety, social, sustainability, technical and financial) and changing environmental factors (e.g. public policy, health and safety) to provide an essential, or critical, service to the nation.
Risk	Risk in the telecommunication sector is the likelihood of a disturbance causing impacts to the viability of the assets and services in the telecommunications sector. Assessments of likelihood and consequence are impacted by degrees of uncertainty. The International Organisation for Standardisation defines risk as the effect of uncertainty on objectives.[87] • An effect is a deviation from the expected • Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. • Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these. • Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence. • In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives. • Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.
Risk acceptance	Informed decision to take a particular risk.[88] • Risk acceptance can occur without risk treatment or during the process of risk treatment. • Accepted risks are subject to monitoring and review.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk.[89] • Risk analysis provides the basis for risk evaluation and decisions about risk treatment. • Risk analysis includes risk estimation.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.[90]

Risk criteria	Terms or reference against which the significance of risk is evaluated.[91] • Risk criteria are based on organizational objectives, and external context and internal context • Risk criteria can be derived from standards, laws, policies and other requirements
Risk evaluation	Process of comparing the results of risk analysis and risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.[92]
Risk identification	Process of finding, recognising and describing risks.[93] • Risk identification involves the identification of risk sources, events, their causes and their potential consequences. • Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.
Telecommunications sector	The purpose of the telecommunications sector is to enable communication to intended recipient through the transmission, reception and/or delivery of information or data (the Purpose). The services provided by the telecommunications sector include network, data, voice, mobile, cloud, and wireless services (Services). The assets that enable these services include physical infrastructure, data centres, networks, and operational port systems (Assets). The sector is made up of those that provide these Services and/or Assets for the Purpose, their supply chains, as well as consumers and regulators.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation.[94]
Uncertainty	Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.[95]
Vulnerabilities	The conditions determined by physical, social, economic, and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards.[96] In common international technology standards, vulnerabilities are classified according to asset class to which they relate: hardware, software, network, personnel, physical and organisational factors.

B. Resilience factors as identified in critical infrastructure resilience literature

The standards and criteria identified in Table 4 are non-exhaustive but indicate that a variety of techniques, qualitative and quantitative methods, simple and complex models and frameworks can be deployed to identify, understand and analyse dependencies and boost resilience characteristics.[97]

Table 4: Resilience factors identified in critical infrastructure literature

Factors	Standards and Criteria	Description
Management/ organisational	Applied sciences and systems, biology and others	Applied physics models, mathematics, biology paradigms, systems theory, epidemiology, sociometry and other similar tools, to help stakeholders with the complexity of CI
	Organisational resilience and governance	The relevance of clear definition for responsible actors to share information
	Performance loss, disruption and recovery process	Performance loss of power systems during a natural disaster, for example, to increase flood resistance and optimise operations through modeling of the electric grid.
	Multiple criteria statistical analysis, monitorisation, predictability and system stability	Multiple criteria statistical process control, patterns and optimal monitorisation to manage incidents in power distribution systems
	Resilience metrics and index	The resilience index for water distribution networks and their performance evaluation
	Statistical distributions, error detection, reliability and/or probability	Error detection of potential cyber-attacks in Supervisory Control And Data Acquisition (SCADA) networks
	Time and demand frequency	Fluctuation of travel time and demand frequency between CI
Safety	Information confidentiality	The vulnerability of the information exchange between CI
	Detection of potential attacks that may prevent success	Protection of SCADA networks from cyber-attacks through cryptographic protocol and leverage of the Cyclic Redundancy Checks
	Safety, security, and risk analysis	Using resilience indicators and cyber security standards as tools to identify risks of CIs and SCADA systems when facing threats such as COVID- 19 and cyber-attacks due to terrorism

Social	Societies/communities resilience and/or social-equity responsibility	Sustainable human settlements and social equity through water and sanitation in rural settlement
	Resilience measured using social media data	Social media data used to measure disaster resilience in power systems
	Resilience through education and professional development	The enhanced resilience of CIs, preparing them to respond when facing a natural disaster
	Socio-economic and socio-political acceptance and evaluation of potential impact	The socio-economic analysis of potential impacts and threats in CIs,
Sustainability	Green infrastructure	Improving urban resilience through GIs
	Life-cycle analysis	Life cycle analysis to examine water infrastructure development in rural settlements or to analyse the resilience of electric power systems
	Resilience through circular economy management	The circular economy used as an innovative proposal for the recycling process of electric vehicle batteries
	Sustainability metrics and environmental vulnerabilities	Technology, economy and environment as metrics for sustainable development in rural settlements and indicators of vulnerability
	Water and sanitisation	Assuring water distribution systems resilience, ensuring water supply and quality distribution in natural disasters prone areas
Technical	Dynamic networks connectivity	The dynamics of airports' network connectivity. The interconnectivity between CIs such as power grids and plants, gas and oil pipelines, among other
	Identification of critical infrastructures	Criteria definition for the identification of CIs
	Innovation and/or regulation	Increasing resilience through using ISO regulations to evaluate potential risks on CIs when facing threats
	Maintenance failures	Failure in maintenance and technical shortcoming is a root cause of catastrophic failure
	Resilience through design and structural integrity	Structural integrity prevention due to natural phenomena
	Real-time control	SCADA systems (Wireless – Mesh- Sensor Networks) used as a critical control system in CIs processes
Financial	Economic Resilience	The reduction of indirect and direct economic losses of power systems.
	Applied sciences and models in business or sectors	The enhancement of business profitability and the application of financial models to invest in local infrastructure safety

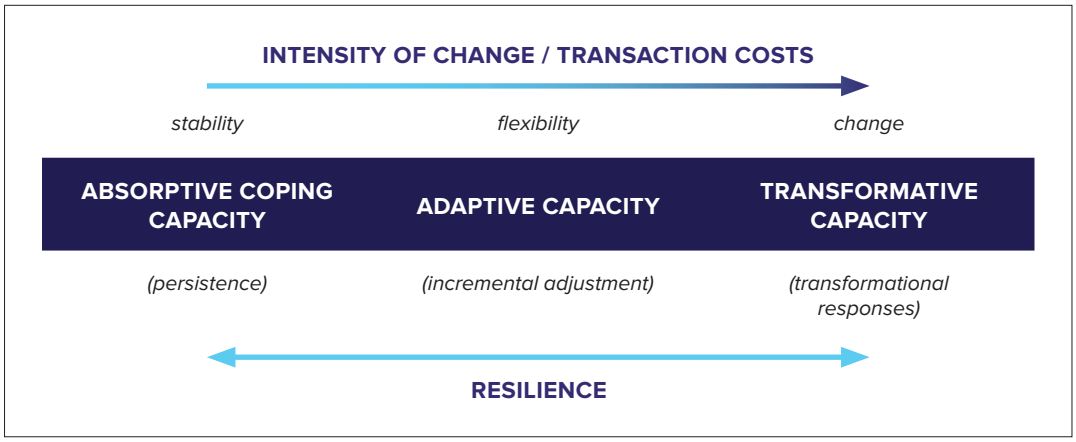
Source: Osei-Kyei et al. (2022)

C. Capacities to boost resilience

Resilience can be boosted by strengthening three different types of capacities:

- **Absorptive coping capacity:** The ability of a system to prepare for, mitigate or prevent negative impacts, using predetermined coping responses to preserve and restore essential basic structures and functions.
- **Adaptive capacity:** The ability of a system to adjust, modify or change its characteristics and actions to moderate potential future damage and to take advantage of opportunities, so that it can continue to function without major qualitative changes in function or structural identity.
- **Transformative capacity:** The ability to create a fundamentally new system so that the shock will no longer have any impact.

Figure 7: The relationship between absorptive, adaptive and transformative capacities for strengthening resilience



Source: OECD Guidelines for Resilience Systems Analysis (2014)

D. Results from initial stakeholder questionnaire

Overview

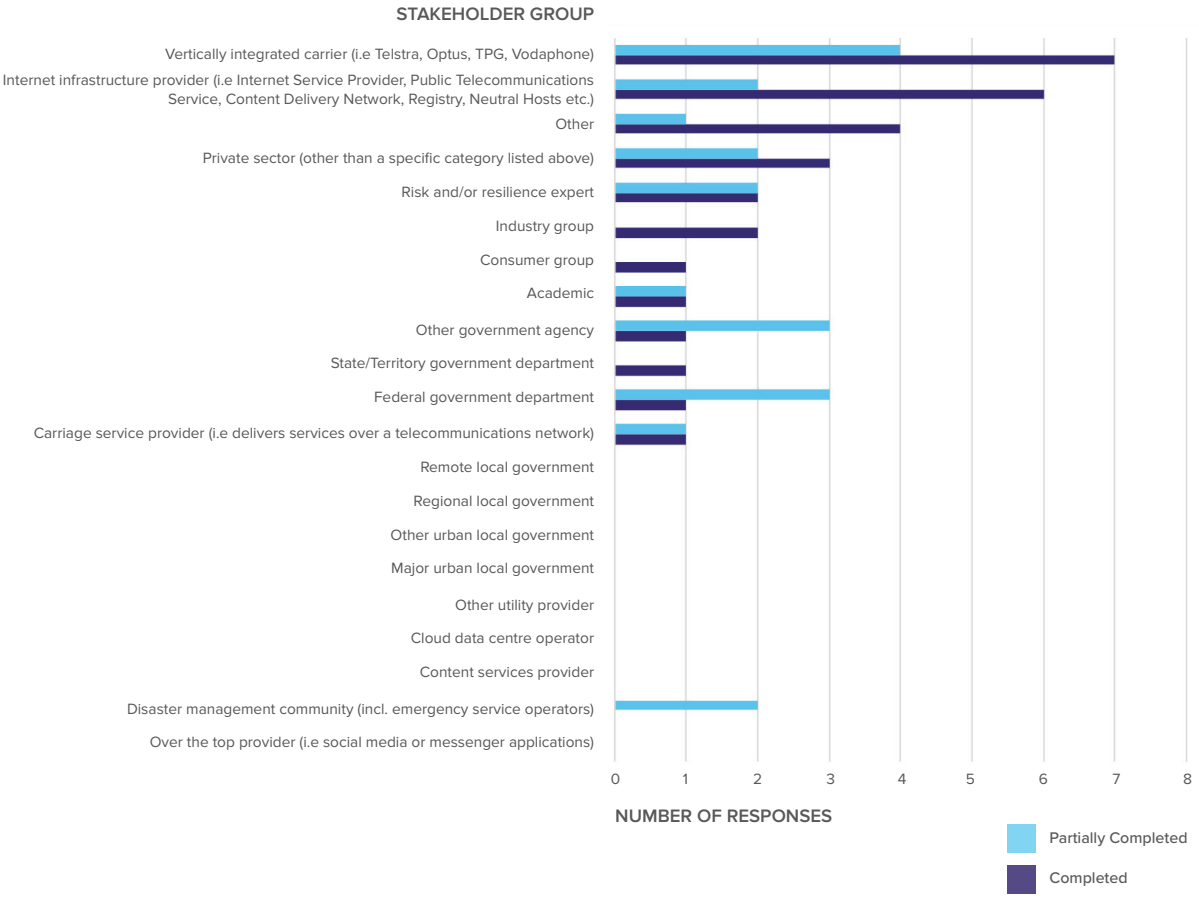
The initial stakeholder questionnaire had 115 total responses (30 fully completed and 85 partial).

The responses from large players, such as vertically integrated carriers and internet infrastructure providers, was strong.

There was an obvious lack of engagement from government departments and agencies at all levels, the cloud industry, utility providers, the disaster and emergency management community, content service providers, and over the top providers.

Through a targeted stakeholder engagement plan, later stages of the project will involve underrepresented stakeholders to ensure all relevant entities inform outputs.

Figure 8: Responses to stakeholder questionnaire – partial and complete



Responses to the question 'is the telecommunication sector resilient?'

Open-ended responses tended to identify scenarios in which resilience was affected. Respondents identified power supply, legacy infrastructure, regulation, information security, extreme weather and third-party organisations as compromising the resilience.

Several responses raised issues with the definition of resilience, the difficulty of measuring it and, given its ambiguity, ensuring appropriate oversight mechanisms to maintain it,. Another response stated it was unlikely that service providers could balance delivering on customer expectations, commercial imperatives and a social good. Representative responses are presented in Table 5.

Table 5: Representative responses to open-ended question "Is the telecommunication sector resilient?

RESPONDENTS	THEME	REPRESENTATIVE STATEMENT/S
Some respondents perceive the telecommunications sector as **resilient**.	**Resilience and adaptability**	'It is resilient to normal every-day conditions.' '[O]verall, the telecommunications sector has demonstrated resilience and adaptability in the face of [recent] challenges.'
The **vast majority** of respondents identified a range of situations that inhibit resilience.	**Sabotage/accident**	'[We] aware of situations where the telecommunications sector has not been resilient, for instance, subsea cables being cut.'
	Power supply	'There is a known critical interdependency between telecommunications and the provision of mains power.'
	Regulatory burden	'[T]he industry experience[s] red tape and regulatory burden regarding whether or not telco is a critical/essential service.'
	Information security	'Information security continues to be concern and the potential ramification such as customer data breaches.'
	Extreme weather/ environmental	[R]ecent extreme examples here in Australia (Fires, Floods, Hacks) and New Zealand (Floods, Cyclones) have shown that networks need to be more resilient moving forward.'
	Legacy infrastructure	'The move away from a copper line phone network has removed a reliable and resilient form of communications (the exchange provided power to household phones).'
	Smaller organisations	'[M]any downstream organisations are unaware of vulnerabilities nor plan for them.'
A **few** respondents perceive the telecommunications sector as **not resilient**.	**Commercial imperatives affect ability to deliver public good**	'Telcos continue to see themselves as corporate entities driven by their own priorities despite them having transitioned into the space of a 'public good' that is a societal enabler. Given the traditional focus, telcos do not fully understand their vulnerabilities. The networks aren't keeping up with expectations consumers have of speedy connectivity because they aren't investing sufficiently to keep pace. Given this, it's unlikely they are investing sufficiently to keep pace with emerging threats.'
	Impossibility of measuring resilience in meaningful way	'Without suitable oversight mechanisms (linking federal, State & Local and across the private and public sectors) resilience in modern tech systems (especially essential services) are close to impossible to attest to.'

Endnotes

1 Savage, G. 2022, Australia needs more than a strategic merchant shipping fleet. *The Strategist*. Australian Strategic Policy Institute. https://www.aspistrategist.org.au/editors-picks-for-2022-australia-needs-more-than-a-strategic-merchant-shipping-fleet/

2 Lin, X.G. et al. 2017, *The development of the sector risk profiling methodology for Australian civil aviation activity and its application to the small aeroplane transport sector*. Civil Aviation Safety Authority. https://www.mssanz.org.au/modsim2017/J5/lin.pdf

3 Organisation for Economic Co-operation and Development (OECD) 2014, *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*. Paris, France: OECD Publishing. https://doi.org/10.1787/3b1d3efe-en

4 Organisation for Economic Co-operation and Development (OECD) 2014, *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*. Paris, France: OECD Publishing. https://doi.org/10.1787/3b1d3efe-en

5 International Organisation for Standardisation [ISO] 2018, *Risk management – Guidelines*. International Organisation for Standardisation. https://www.iso.org/iso-31000-risk-management.html

6 International Organisation for Standardisation [ISO] 2018, *Information Technology – Security techniques – information security management systems – Overview and vocabulary*. https://www.iso.org/standard/73906.html

7 International Organisation for Standardisation [ISO] 2018, *Information Technology – Security techniques – information security management systems – Overview and vocabulary*. https://www.iso.org/standard/73906.html

8 Pursiainen, C., & Kytömaa, E 2023, From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85-101. doi: 10.1080/23789689.2022.2128562

9 Pursiainen, C., & Kytömaa, E 2023, From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure,* 8(sup1), 85-101. doi: 10.1080/23789689.2022.2128562

10 Organisation for Economic Co-operation and Development (OECD) 2014, *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*. Paris, France: OECD Publishing. https://doi.org/10.1787/3b1d3efe-en

11 National Academy of Sciences (NAS) Committee on Science, Engineering, and Public Policy 2012, *Disaster Resilience: A National Imperative*. The National Academies Press. https://nap.nationalacademies.org/catalog/13457/disaster-resilience-a-national-imperative

12 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, doi: 10.1109/37.969131

13 Liu W, Shan M, Zhang S, Zhao X, Zhai Z 2022, Resilience in Infrastructure Systems: A Comprehensive Review. *Buildings*, 12(6):759. https://doi.org/10.3390/buildings12060759

14 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. doi: 10.1109/37.969131

15 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

16 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

17 See for example, Section 52B(2) of the SOCI Act; Home Affairs 2020, *Protecting Critical Infrastructure Systems of National Significance Consultation Paper*. Australian Government. https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

18 Osei-Kyei et al. 2022, Systematic review of critical infrastructure resilience indicators. *Construction Innovation*. https://doi.org/10.1108/CI-03-2021-0047

19 Linkov, I, Trump, B, Hynes, W 2019, *Resilience Strategies and Approaches to Contain Systemic Threats*. OECD Publishing. https://www.oecd.org/naec/averting-systemic-collapse/SG-NAEC(2019)5_Resilience_strategies.pdf

20 Australian Government Treasury 2021, *Telecommunications Sectoral Assessment - Consultation Paper*. Australian Government Treasury. https://treasury.gov.au/sites/default/files/2021-07/182135_telecommunicationssectoralassessment-consultationpaper.pdf

21 Australian Bureau of Statistics n.d, *Information Media and Telecommunications Services*. https://www.abs.gov.au/ausstats/abs@.nsf/mf/8681.0

22 Department of Communications and the Arts, Bureau of Communications Research 2016, *The communications sector, recent trends and developments*. Australian Government. https://www.infrastructure.gov.au/sites/default/files/the-communications-sector-recent-trends-and-developments.pdf

23 *Security of Critical Infrastructure Act* 2018, Part 2A

24 *Security of Critical Infrastructure Act* 2018, Part 2A

25 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. doi: 10.1109/37.969131

26 Australian Competition and Consumer Commission 2016, *How access to infrastructure services is regulated*. https://www.accc.gov.au/by-industry/regulated-infrastructure/how-access-to-infrastructure-services-is-regulated

27 Madsen, A, & De Percy, M 2020, Telecommunications infrastructure in Australia. *Australian Journal of Social Issues*, 55(2), 218-238. doi: 10.1002/ajs4.121

28 Productivity Commission 2001, *Telecommunications Competition Regulation*. Australian Government. https://www.pc.gov.au/inquiries/completed/telecommunications-competition/report/telecommunications3.pdf

29 Regional Telecommunications Review 2021, *Regional Telecommunications Review 2021: Issues Paper*. https://www.infrastructure.gov.au/sites/default/files/documents/regional-telecommunications-review-2021-issues-paper.pdf

30 Department of Home Affairs and Department of Communications and the Arts 2018, *Government provides 5G security guidance to Australian carriers*. Australian Government. https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22

31 City of Melton 2017, *Background Analysis Paper: Communications Infrastructure Policy*. https://www.melton.vic.gov.au/Services/Building-Planning-Transport/Strategic-Planning/Studies-Strategies-Guidelines/Communications-Infrastructure-Policy-Framework

32 Australian Trade and Investment Commission n.d, *Data Tool: Foreign-owned businesses in Australia*. Australian Government. https://www.austrade.gov.au/international/invest/importance-of-foreign-direct-investment/economic-activity-of-foreign-owned-businesses-in-australia

33 Tech Council of Australia 2022, *Submission in response to the 2022 Foreign Investment Reforms – Discussion Paper*. Tech Council of Australia. https://treasury.gov.au/sites/default/files/2023-04/c2022-244363-techcouncilofaustralia.pdf

34 Productivity Commission 2022, *5 Year Productivity Inquiry: Innovation for the 98%*. Australian Government. https://www.pc.gov.au/inquiries/completed/productivity/interim3-innovation

35 Department of Home Affairs and Department of Communications and the Arts 2018, *Government provides 5G security guidance to Australian carriers*. Australian Government. https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22

36 European Parliamentary Research Service 2022, *'Splinternets': Addressing the renewed debate on internet fragmentation*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf; Council on Foreign Relations 2022, Independent Task Force Report No. 80: Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. Council on Foreign Relations. https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace

37 EuroStat. n.d, *What is the digital single market about?* European Parliament. https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

38 Sacco, F.M 2020, The Evolution of the Telecom Infrastructure Business. In: Gatti, S., Chiarella, C. (eds) *Disruption in the Infrastructure Sector: Future of Business and Finance*. Springer, Cham. doi: 10.1007/978-3-030-44667-3_4

39 International Monetary Fund (IMF) 2023, *World Economic Outlook*. https://www.imf.org/en/Publications/WEO#:~:text=Global%20inflation%20is%20expected%20to,still%20above%20pre%2Dpandemic%20levels

40 Australian Broadband Advisory Council 2020, *Riding The Digital Wave: Report on COVID19 Trends and Forward Work Program*. https://www.infrastructure.gov.au/sites/default/files/riding-the-digital-wave-report-on-covid-19-trends-and-forward-work-program.pdf

41 ACMA 2022, *How we communicate*. https://www.acma.gov.au/sites/default/files/2023-03/How%20we%20communicate_Executive%20summary%20and%20key%20findings_0.pdf

42 Gaibi, Z et al. 2021, *A blueprint for telecom's critical reinvention*. McKinsey. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/a-blueprint-for-telecoms-critical-reinvention

43 Reserve Bank of Australia 2021, *The Evolving Payments Landscape Payments System Board Annual Report – 2021*. https://www.rba.gov.au/publications/annual-reports/psb/2021/the-evolving-payments-landscape.html

44 Tech Council of Australia 2022, *Australia's Tech Jobs Opportunity – Cracking the Code to Australia's Best Jobs*. https://techcouncil.com.au/wp-content/uploads/2022/03/2022-Tech-Jobs-Opportunity-report.pdf

45 Tech Council of Australia 2022, *Getting to 1.2 million: Our roadmap to create a thriving Australian tech workforce*. https://techcouncil.com.au/wp-content/uploads/2022/08/2022-Getting-to-1.2-million-report.pdf

46 Labour Market Insights 2022, *Information Media and Telecommunications*. Australian Government. https://labourmarketinsights.gov.au/industries/industry-details?industryCode=J

47 National Skills Commission 2022, *Skills Priority List*. Australian Government. https://www.nationalskillscommission.gov.au/topics/skills-priority-list

48 PWC 2022, *Australian Telecommunications, Media and Technology Outlook*. https://www.pwc.com.au/industry/telecommunications/assets/2022-australian-tmt-outlook.pdf

49 Lifshitz-Assaf, H and Nagle, F 2021, *The Digital Economy Runs on Open Source. Here's How to Protect It*. Harvard Business Review. https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it

50 Department of Infrastructure, Transport, Regional Development, Communications and the Arts n.d, *Mobile Black Spot Program*. Australian Government. https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-services-and-coverage/mobile-black-spot-program

51 Department of Infrastructure, Transport, Regional Development, Communications and the Arts n.d, *Better Connectivity Plan for Regional and Rural Australia*. https://www.infrastructure.gov.au/media-communications-arts/better-connectivity-plan-regional-and-rural-australia

52 Ericsson 2022, *Telstra deploys industry-first Ericsson Private 5G for enterprise*. https://www.ericsson.com/en/press-releases/7/2022/telstra-deploys-industry-first-ericsson-private-5g-for-enterprise

53 Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2021, *Universal Service Guarantee (USG)*. Australian Government. https://www.infrastructure.gov.au/sites/default/files/documents/universal-service-guarantee-usg-3september2021.pdf

54 Productivity Commission 2017, *Telecommunications Universal Service Obligation Inquiry Report: Overview and Recommendations*. Australian Government. https://www.pc.gov.au/inquiries/completed/telecommunications/report/telecommunications-overview.pdf

55 Regional Telecommunications Review 2021, *Regional Telecommunications Review 2021: Issues Paper*. https://www.infrastructure.gov.au/sites/default/files/documents/regional-telecommunications-review-2021-issues-paper.pdf

56 Roy Morgan 2022, *A majority of Australians have no trust in telcos*. https://www.roymorgan.com/findings/a-majority-of-australians-have-no-trust-in-telcos

57 *Edelman Trust Barometer Australia Report 2023*. https://www.edelman.com.au/sites/g/files/aatuss381/files/2023-02/2023%20Edelman%20Trust%20Barometer%20Report%20-%20AUS%2002-2023.pdf

58 Department of Infrastructure, Transport, Regional Development, Communications and the Arts and the National Emergency Management Agency 2022, *Better communications to keep communities safer in disasters*. Australian Government. https://minister.infrastructure.gov.au/rowland/media-release/better-communications-keep-communities-safer-disasters

59 ACCC 2022, *Regional mobile infrastructure inquiry 2022-23*. https://www.accc.gov.au/inquiries-and-consultations/regional-mobile-infrastructure-inquiry-2022-23

60 ACCC 2022, *Regional mobile infrastructure inquiry 2022-23*. https://www.accc.gov.au/inquiries-and-consultations/regional-mobile-infrastructure-inquiry-2022-23

61 ACMA 2020, *Impacts of the 2019-20 bushfires on the telecommunications network*. https://www.acma.gov.au/publications/2020-04/report/impacts-2019-20-bushfires-telecommunications-network

62 Royal Commission into National Natural Disaster Arrangements 2020, *Final Report*. Australian Government. https://naturaldisaster.royalcommission.gov.au/final-report

63 United Nations Office for Disaster Risk Reduction (UNDRR) 2020, *Global Assessment Report on Disaster Risk Reduction – Special Report on Drought 2021*. Geneva, Switzerland: United Nations Office for Disaster Risk Reduction (UNDRR). https://council.science/wp-content/uploads/2020/06/UNDRR_Hazard-Report_DIGITAL.pdf

64 International Organisation for Standardisation [ISO] 2018, *Information Technology – Security techniques – information security management systems – Overview and vocabulary*. https://www.iso.org/standard/73906.html

65 Sacco, F.M 2020, The Evolution of the Telecom Infrastructure Business. In: Gatti, S., Chiarella, C. (eds) *Disruption in the Infrastructure Sector: Future of Business and Finance*. Springer, Cham. doi: 10.1007/978-3-030-44667-3_4

66 GSMA 2023, *Post Quantum Telco Network Impact Assessment Whitepaper Version 1.0.* https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf

67 *Security of Critical Infrastructure Act* 2018, Part 2A

68 *Commonwealth of Australia Constitution Act* 1900 (Cth), section 51(v)

69 Department of the Prime Minister and Cabinet 2021, *Australian Government Crisis Management Framework (AGCMF)*. Australian Government. https://www.pmc.gov.au/publications/australian-government-crisis-management-framework-agcmf

70 CSIRO n.d, Climate Change Information. https://www.csiro.au/en/research/environmental-impacts/climate-change/climate-change-information

71 Intergovernmental Panel on Climate Change 2021, Summary for Policymakers. *IPCC Working Group I Contribution to AR6*. https://www.ipcc.ch/report/ar6/wg1/downloads/report/IPCC_AR6_WGI_Chapter04.pdf

72 International Energy Agency 2020, *Global Energy and Climate Model: Model Description*. https://www.iea.org/reports/global-energy-and-climate-model

73 Murray, L.T, Pope, J.O, & Arnold, S.R 2022, A global compilation of atmospheric sulfur dioxide measurements: 1964–2020. *Earth-Science Reviews*, 229, 103778. https://www.sciencedirect.com/science/article/pii/S0012825222003804

74 Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2023, *Release of the Public Safety Mobile Broadband Review and the Government Response*. Australian Government. https://www.infrastructure.gov.au/department/media/news/release-public-safety-mobile-broadband-review-and-government-response

75 Department of Infrastructure, Transport, Regional Development, Communications and the Arts 2023, *Release of the Public Safety Mobile Broadband Review and the Government Response*. https://www.infrastructure.gov.au/department/media/news/release-public-safety-mobile-broadband-review-and-government-response

76 Royal Commission into National Natural Disaster Arrangements 2020, *Final Report.* Australian Government. https://naturaldisaster.royalcommission.gov.au/final-report

77 OECD 2008, Protection of *'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. http://www.oecd.org/daf/inv/investment-policy/40700392.pdf

78 Pescaroli, G, & Alexander, D 2018, Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. *Risk Analysis*, 38(12), 2247-2259. doi: 10.1111/risa.13128

79 Pescaroli, G, & Alexander, D 2018, Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. *Risk Analysis*, 38(12), 2247-2259. doi: 10.1111/risa.13128

80 ISO/IEC 2018, *Risk management – Guidelines. International Organisation for Standardisation*. https://www.iso.org/iso-31000-risk-management.html

81 ISO/IEC 2018, *Risk management – Guidelines. International Organisation for Standardisation*. https://www.iso.org/iso-31000-risk-management.html

82 National Academy of Sciences (NAS) Committee on Science, Engineering, and Public Policy 2012, *Disaster Resilience: A National Imperative*. The National Academies Press. https://nap.nationalacademies.org/catalog/13457/disaster-resilience-a-national-imperative

83 National Academy of Sciences (NAS) Committee on Science, Engineering, and Public Policy 2012, *Disaster Resilience: A National Imperative*. The National Academies Press. https://nap.nationalacademies.org/catalog/13457/disaster-resilience-a-national-imperative

84 National Academy of Sciences (NAS) Committee on Science, Engineering, and Public Policy 2012, *Disaster Resilience: A National Imperative*. The National Academies Press. https://nap.nationalacademies.org/catalog/13457/disaster-resilience-a-national-imperative

85 European Commission 2017, *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions*. https://ec.europa.eu/energy/sites/ener/files/documents/communication_resilience_en.pdf

86 European Commission 2017, *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions.* https://ec.europa.eu/energy/sites/ener/files/documents/communication_resilience_en.pdf

87 Pursiainen, C & Kytömaa, E 2023, From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85-101. doi: 10.1080/23789689.2022.2128562

88 Pursiainen, C & Kytömaa, E 2023, From European

critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, 8(sup1), 85-101. doi: 10.1080/23789689.2022.2128562

89 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

90 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

91 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. doi: 10.1109/37.969131

92 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, doi: 10.1109/37.969131

93 European Commission 2017, *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions*. https://ec.europa.eu/energy/sites/ener/files/documents/communication_resilience_en.pdf

94 European Commission 2017, *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions*. https://ec.europa.eu/energy/sites/ener/files/documents/communication_resilience_en.pdf

95 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

96 Critical Infrastructure Security Centre 2023, *Critical Infrastructure Resilience Strategy*. https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy

97 Rinaldi, et al. 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. doi: 10.1109/37.969131

Australian National University

TECH POLICY DESIGN CENTRE

Tech Policy Design Centre
Australian National University
E: techpolicydesign@anu.edu.au
W: www.techpolicydesign.au
TPDesignCentre