Australian National University | NATIONAL SECURITY COLLEGE

OCCASIONAL PAPER AUGUST 2026

Connected & protected

Building Australia's submarine cable resilience

David Brewster, Samuel Bashfield, Jocelinn Kang,
Mike Constable and Anthony Bergin

Cover image: The cable-laying ship Ile de Brehat landing the Coral Sea Cable at Tamarama Beach, Sydney, in 2019. Source: DFAT

ANU National Security College
national.security.college@anu.edu.au

The Australian National University Canberra ACT 2600 Australia
www.anu.edu.au

CRICOS Provider No. 00120C
TEQSA Provider ID: PRV12002 (Australian University)

About the authors

Dr David Brewster is a Senior Research Fellow with the ANU National Security College. He is one of Australia's leading experts on Indian Ocean maritime security and is the author of many books, reports, and papers on that subject.

Dr Samuel Bashfield is Research Fellow at the La Trobe Centre for Global Security, where he studies geopolitics and defence trends. He speaks and publishes on national security and defence issues in leading international disciplinary journals and influential media outlets. His research examines how Australia and its partners respond to global geopolitical developments, new technologies and changing power distributions, with particular focus on maritime security, digital flows, and Indo-Pacific strategic dynamics. He is the author of *Submarine Cables* (Cambridge Elements in Indo-Pacific Security, 2026).

Ms Jocelinn Kang is the founder of Nodalys, a boutique technology and national security consultancy that aims to strengthen digital resilience through research, advisory and training. Originally trained as a computer systems and network engineer, she held multiple roles in the Australian Department of Defence and the Department of Foreign Affairs and Trade before joining the Australian Strategic Policy Institute as a technical specialist and program manager, where she shaped government and industry understanding of cyber and technology policy issues.

Mr Mike Constable is a senior executive with 30 years in the submarine cable industry, having held prominent leadership roles in both investment and supply-side sectors. He is founder of Infra-Analytics, a strategic advisory consultancy and serves as Vice Chairman of the UN Joint Task Force on SMART cables. Recognised as an authority in his field, he regularly contributes as a speaker and thought leader on regulatory and geopolitical matters, market trends, submarine cable investment and operations. He holds undergraduate and MBA degrees and completed the Advanced Management Programme at Harvard Business School.

Dr Anthony Bergin is an Expert Associate at the ANU National Security College. He was formerly the Research Director and Deputy Director at the Australian Strategic Policy Institute. He holds a doctorate on the law of the sea. Dr Bergin has been a consultant to a wide range of public- and private-sector clients on matters related to maritime security. In 2022, he co-directed (with David Brewster) a baseline study for DFAT on regional arrangements in marine ecology in the Indo-Pacific. He recently collaborated with Dr Brewster on reports focused on maritime security in Sri Lanka and Bangladesh. He is the author of numerous academic articles and think-tank reports on Indo-Pacific maritime affairs.

About this paper

Occasional Papers comprise peer-reviewed research on subjects of national security significance, written by academics, policy practitioners and subject-matter experts affiliated with the ANU National Security College. Justin Burke is the series editor and Senior Policy Advisor at NSC.

About the College

The ANU National Security College (NSC) is a joint initiative of The Australian National University and the Australian Government. NSC offers specialised professional development and postgraduate degrees; futures analysis; and a hub for expertise, dialogue and networks on national security policy.

Contents

Executive summary and recommendations

1. The problem

1.1 ***Critical infrastructure:*** Australia now depends on some 16 privately operated submarine cables for the vast majority of its international communications and data needs. The smooth functioning of this network is critical to Australia's economy, society and national security. In coming years, Australia will likely grow ever more reliant on this infrastructure (see Section 1).

1.2 ***Opportunity for Australia to be an Indo-Pacific cables hub:*** the international submarine cable industry is undergoing significant changes, driven by geopolitical tensions, 'hyperscaler' investment, and surging data demand. These developments are redrawing new Indo-Pacific cable routes away from the South China Sea and Malacca Strait, positioning Australia as a preferred alternative hub. This is a significant economic and strategic opportunity, but one that requires the right policy settings to capture the benefit (see Section 2).

1.3 ***Growing threats to submarine cables:*** submarine cables are highly vulnerable to a range of human and environmental threats. In recent years, there have been numerous incidents of disruption to cables, at least some of which are suspected to be intentional attacks. Submarine cables are likely to be a high-priority target for an adversary in any conflict (see Section 5.3).

1.4 ***Lack of strategic guidance:*** despite their critical strategic importance, the security of submarine cables receives little or no mention in Australia's key strategic documents such as the *2026 National Defence Strategy* or the *2022 Civil Maritime Security Strategy* (see Section 4.1).

1.5 ***Lack of comprehensive strategy:*** Australia lacks a comprehensive strategy to properly protect and govern its submarine cable networks, to respond to a range of threats, or to take full advantage of economic opportunities. Policy settings that enhance security are also the settings that attract investment (see Section 9).

1.6 ***Lack of clear allocation of responsibilities among relevant agencies:*** many federal and state government agencies have roles in governing Australia's submarine cables. There is no clear governmental statement on the responsibilities of relevant agencies or formal mechanisms for coordination among relevant agencies, either at a policy or operational level (see Section 4).

1.7 ***Protection from physical and cyber-attack:*** due to their offshore and underwater location, it is difficult to protect submarine cables from physical attack. Cyber-attacks, especially those targeting the equipment at terrestrial interconnection points, could cause a significant, prolonged outage. Protecting cables from deliberate state-based attack ultimately requires military as well as civil capabilities – including seabed surveillance, anti-submarine warfare (ASW), counter-uncrewed underwater vehicle (UUV), and clearance diving – areas where Australia has significant gaps (see Sections 5 and 6).

1.8 ***Repair capabilities:*** foreign private operators are responsible for repairs to all cables connected to Australia. The Australian Government has no way of ensuring swift repair response even in cases of national emergency (see Section 7).

1.9 ***Need for international cooperation:*** submarine cables must be protected along their entire length. By their nature, international submarine cables will cross numerous jurisdictions, as well as international jurisdiction (high seas), requiring Australian cooperation with international partners (see Section 8).

1.10 ***Gaps in the legal regime:*** there are significant inadequacies in Australia's legal regime for the protection of submarine cables, including inadequate regulatory authority to mitigate risks as well as significant gaps in the ability of law enforcement authorities to act against persons who disrupt submarine cables inside and outside areas of direct Australian jurisdiction (see Section 4).

2. Recommendations for priority actions

We make the following recommendations for priority actions to mitigate risks and vulnerabilities in Australia's submarine cables network. Because these recommendations are interrelated, they are not listed here in priority order:

2.1 ***Update strategic guidance:*** Australia's *National Defence Strategy*, *Civil Maritime Security Strategy*, *Cyber Security Strategy*, and the *Guide to Australian Maritime Security Arrangements* should be updated to provide guidance to the national security community on addressing threats to the country's submarine cables network.

2.2 ***Designate Maritime Border Command as lead coordinating agency on physical threats:*** the Australian Border Force (ABF), and specifically Maritime Border Command (MBC), should be designated as the lead coordinating agency for monitoring and securing Australia's submarine cable network from physical disruption or attacks within Australia's Security Forces Authority Area, including terrestrial infrastructure up to cable landing stations. MBC would be supported by the Australian Defence Force (ADF) and other relevant federal and state agencies. To fulfil this function, MBC would need to have access to adequate resourcing and personnel.

2.3 ***Designate Australian Signals Directorate as lead technical authority on cyber threats:*** the Australian Signals Directorate (ASD) should be designated as the lead technical authority for cyber threat intelligence, advice and incident response in respect of Australia's submarine cables network, working directly with cable operators and supported by appropriate agencies.

2.4 ***Designate an interagency coordination mechanism for cables:*** the Australian Government should designate the Joint Agencies Maritime Advisory Group (JAMAG) or another committee as the high-level interagency coordination committee with principal responsibility for the coordination of policy and operational responses among relevant agencies in respect of submarine cables. The committee should report regularly to the Secretaries Committee on National Security on threat developments and cable network security.

2.5 ***Establish industry advisory board and liaisons:*** the Australian Government should establish an advisory board including Australian cable network operators and other industry stakeholders to work with the interagency coordination committee. Key agencies such as MBC, the ADF, and ASD should also establish and/or maintain direct liaisons with private cable operators.

2.6 ***Ensure ADF capabilities keep pace with evolving cable threats:*** the ADF should ensure that capabilities relevant to the protection of submarine cable infrastructure are adequate to the modern threat environment, including seabed surveillance and maritime domain awareness, ASW, counter-UUV capabilities, as well as clearance diving and counter-mine warfare.

2.7 ***Promote new monitoring and surveillance technologies:*** The Australian Communications and Media Authority (ACMA) should have the power to mandate that newly-installed cable systems be complemented by monitoring technologies to monitor proximate objects and events, including vessel activities.

2.8 ***Ensure Network Operations Centres meet Australian jurisdictional and security requirements:*** operators should be required to locate a primary Network Operations Centre (NOC), or a remote access facility with overall network management capability, within Australia. This would ensure that cable network operations are subject to Australian jurisdictional and security requirements.

2.9 ***Establish new cable protection zones:*** ACMA should declare new cable protection zones (CPZs) in the Northern Territory, Queensland, and elsewhere as part of a strategy of diversifying cable landing sites and routes.

2.10 ***Priority access to repairs*:** the Australian Government should establish arrangements that would let relevant authorities trigger priority access to repair capabilities in case of national emergency. This would also require timely access to spares.

2.11 ***Promote the establishment of an Indo-Pacific industry association*:** the Australian Government should promote the establishment of an Indo-Pacific cable industry association as a forum for regional operators to cooperate in mitigating risks.

2.12 ***Continue funding DFAT's Cable Connectivity and Resilience Centre and the Australian Infrastructure Financing Facility for the Pacific***: the Australian Government should continue funding for DFAT's Cable Connectivity and Resilience Centre, and to ensure the Australian Infrastructure Financing Facility for the Pacific (AIFFP) continues supporting submarine cable projects in the Pacific.

2.13 ***Convene an Indo-Pacific conference on cable security:*** DFAT's Cable Connectivity and Resilience Centre should consider convening an international conference with Indo-Pacific partner states and regional cable operators to clarify legal responsibilities, develop common standards, and develop shared responses to threats and incidents.

2.14 ***Learn from European partners:*** DFAT should lead a step-up in Australia's engagement with European partners to exchange views on response protocols, challenges and identify potential areas of policy cooperation.

2.15 ***Parliamentary inquiry on submarine cables***: the security and resilience of Australia's submarine cable network should be the subject of a parliamentary inquiry. This would examine how to facilitate civil and Defence assets working with industry to strengthen the resilience of Australia's cable network and consider gaps in legal and regulatory frameworks that might impede the ability for law enforcement, Defence, and security agencies to prevent and respond to any disruptions to Australia's cables. A public inquiry would be a valuable way of driving significant organisational and legal reform.

3. Recommendations for a comprehensive submarine cable resilience strategy

Australia needs a comprehensive cable resilience strategy that includes the following elements (see Section 9):

3.1 ***Digital Infrastructure Investment Policy:*** include policies to actively promote Australia as the Indo-Pacific's preferred cable hub, recognising that attracting new cable investment directly enhances digital resilience.

3.2 ***Identify threats and mitigation strategies:*** identify potential threats and vulnerabilities to Australia's cables network, major risk scenarios, and potential mitigation strategies.

3.3 ***Allocate responsibilities among relevant agencies:*** allocate responsibilities for cable network security among relevant federal and state agencies, including the designation of agencies in leading and supporting roles in respect of specified threats.

3.4 ***Interagency policy and operational coordination mechanisms:*** designate JAMAG or another committee as the principal high-level interagency coordination committee among relevant agencies to coordinate policy and operational responses.

3.5 ***Government-private operator coordination mechanism***: the strategy should establish an advisory board including Australian cable network operators and other industry stakeholders that would support the interagency committee as well as informing relevant line agencies.

3.6 ***Resourcing of responsible agencies:*** include commitments to adequately resource relevant agencies – particularly MBC and the ADF – to fulfil designated responsibilities.

3.7 ***Update the legal and security regime:*** include a commitment to undertake a review of Australia's legal regime for the protection of submarine cables to ensure that regulatory authorities have adequate powers to require private operators to mitigate threats, and that law enforcement authorities have necessary powers to act against persons or vessels that seek to disrupt Australia's submarine cable network.

3.8 ***Enhance physical cable protection and promote monitoring and surveillance capabilities:*** set out policies for the deployment of physical cable protection measures, enhanced monitoring and surveillance, and the integration of ADF capabilities into cable protection – including seabed surveillance, ASW, counter-UUV, and clearance diving and mine countermeasures.

3.9 ***Enhancing cable redundancy and geographic and ownership diversity:*** the strategy should provide a framework for enhancing investment in Australia's submarine cables network to promote redundancy and geographic diversity, as well as diversity in cable owners and operators. The strategy should consider how to encourage and sustain a viable cohort of Australian-owned operators.

3.10 ***Ensuring timely access to cable repair capabilities:*** set out approaches for ensuring timely access to cable repair capabilities (including specialist workforce, equipment, and spares) in cases of national emergency. This may include a mix of sovereign capabilities and stockpiles and arrangements for priority access to private capabilities.

3.11 ***Ensuring access to satellite connectivity:*** ensure there is adequate access to satellite communications connectivity as a partial back-up in case of widespread disruption to Australia's cables network. This would require accountability for funding and clear understandings on traffic prioritisation.

3.12 ***Mitigating cyber risks:*** cyber-attack may be one of the greatest threats faced by Australia's cables network. The strategy should designate ASD as the lead technical authority for cyber threat intelligence, advice and incident response. Moreover, the strategy should require new cables be built secure-by-design and mandate cyber security exercises and vulnerability assessments.

3.13 ***Regional and international engagement strategies:*** set out a regional engagement strategy with partners in Southeast Asia, the Pacific and Indian oceans, and a broader international engagement strategy for capability building and coordinated incident response with key partners, underpinned by continued funding for DFAT's Cable Connectivity and Resilience Centre and the AIFFP.

3.14 ***Connecting Antarctica:*** include an Australian Government commitment to developing cable connectivity with Australia's research stations in Antarctica.

3.15 ***Related seabed infrastructure:*** the strategy should address the protection of related seabed infrastructure, including power cables, pipelines and other critical seabed assets.

3.16 ***Deterrence doctrine:*** indicate Australia's approach to deterring potential adversaries from disrupting Australia's submarine cables network. Effective deterrence requires demonstrated detection and attribution capability, clear response thresholds, and a willingness to impose costs on those who attack Australian infrastructure, which must be developed and exercised in close coordination with allies.

Contributors

Dr Tony Press is Adjunct Professor with the Australian Antarctic Program Partnership, Institute for Marine and Antarctic Studies, University of Tasmania. In former roles he was Director of the Australian Antarctic Division (1998–2009); Australian Delegate and often Head of Delegation to Antarctic Treaty Consultative Meetings (1999–2008); Australian Commissioner to the Commission for the Conservation of Antarctic Marine Living Resources (1998–2008); and Chair of the Antarctic Treaty Committee for Environmental Protection (2002–06). He was chief executive of the Antarctic Climate and Ecosystems Cooperative Research Centre (2009–14). In 2014, he delivered the 20-Year Australian Antarctic Strategic Plan to the Australian Government.

Dr Amanda H A Watson has established a reputation as the leading expert on digital technologies and infrastructures in the Pacific Islands region. Dr Watson's expertise includes undersea internet cables, satellite internet services and telecommunications in the Pacific. She is actively engaged in monitoring, analysing and commenting on telecommunication sector regulatory processes and developments in the Pacific. She has a particular interest in mobile telephone uptake and use in Papua New Guinea (PNG). Her multi-year project with academic partners in PNG monitors mobile internet prices. Dr Watson is a Fellow at the Department of Pacific Affairs at the Australian National University.

Acknowledgements

Connected & protected was produced with funding support from the Australian Department of Defence, as part of Strategic Policy Grant Program project '053-2024 – Defending Seabed Critical Infrastructure'. The authors would like to acknowledge the assistance of the many anonymous reviewers from government agencies, the submarine cable industry and academia in reviewing earlier drafts of this report. All perspectives and errors contained in this report are the authors' own.

Key acronyms and abbreviations

ACMA	Australian Communications and Media Authority
ABF	Australian Border Force
ADF	Australian Defence Force
AIFFP	Australian Infrastructure Financing Facility for the Pacific
APMMSA	Asia-Pacific Marine Maintenance Service Agreement
AIS	Automatic Identification System
ASD	Australian Signals Directorate
BMH	beach manhole
CS2	Coral Sea Cable System
CLS	cable landing station
DAS	distributed acoustic sensing
DFAT	Department of Foreign Affairs and Trade
DITRDCSA	Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
EEZ	Exclusive Economic Zone
IRU	indefeasible right of use
ICT	information and communication technology
IFC	information fusion centre
ICPC	International Cable Protection Committee
ISR	intelligence, surveillance, and reconnaissance
LEO	low Earth orbit
MBC	Maritime Border Command
MDA	maritime domain awareness
NMS	Network Management System
NOC	Network Operations Centre
OFC	optical fibre communication
PNG	Papua New Guinea
SEAIOCMA	South East Asian Indian Ocean Cable Maintenance Agreement
SOCI	Security of Critical Infrastructure (Act)
Tbps	terabits per second
UNCLOS	United Nations Convention on the Law of the Sea
US	United States
UUV	uncrewed underwater vehicle

Introduction

"The seabed is becoming a battlefield … And we have been slow – collectively slow – to recognise [submarine cables] as the strategic targets they have become."

The Hon Richard Marles MP, Deputy Prime Minister and Minister for Defence, Australia, Shangri-La Dialogue, Singapore, 30 May 2026.[1]

Connected & protected provides a comprehensive assessment of Australia's submarine cables network. It sets out recommendations to promote our economic interests and secure our submarine cables network from key threats and vulnerabilities. Australia currently depends on some 16 privately operated submarine cables for the vast majority (around 99 per cent) of its international communications and data needs. The smooth functioning of these cables is critical to Australia, as any significant network disruption would likely have widespread adverse consequences for its economy, society, and national security.

The international submarine cable industry is undergoing significant change, driven by a combination of factors. Geopolitical concerns are leading to a bifurcation of the industry between Chinese and non-Chinese players as well as the re-routing of cables outside of sensitive areas. Meanwhile, so-called 'hyperscaler' technology companies, including Google and Meta, with massively increased data transmission and processing needs, are driving major new investments.

Together, these are changing the shape of the Indo-Pacific cable network and presage significant new investment in Australia's cables. These developments are creating a significant opportunity for Australia. Its geography, political stability, and status as a trusted network partner are attracting cable investment that previously transited through what are now increasingly geopolitically sensitive chokepoints. Australia's digital resilience and its economic interests are therefore well served by actively positioning itself as an Indo-Pacific preferred cable hub. That requires ensuring our domestic policy settings are conducive to that role.

Submarine cables face growing threats from state and non-state adversaries. As recent incidents in European and Indo-Pacific waters have shown, cables can be disrupted as part of a strategy of hybrid/grey-zone warfare, and Australia's communications history demonstrates that its cables would be a high-priority target in any major conflict.

But, due to their offshore and underwater location, it is difficult to protect submarine cables from physical attack, including from ships' anchors, grapnels, and UUVs. Submarine cables are also highly vulnerable to cyber-attack both on land and at sea. Protecting cables from deliberate state-based attack ultimately requires military as well as civil capabilities – including seabed surveillance, ASW, counter-UUV, mine countermeasures and clearance diving – areas where Australia currently has gaps.

Despite its critical importance to Australia, the security of submarine cables receives little or no mention in Australia's key strategic documents such as the *2026 National Defence Strategy*, the *2022 Civil Maritime Security Strategy*, or the *2023-2030 Australian Cyber Security Strategy*. Consistent with this lack of high-level strategic guidance, Australia does not currently have a clear and comprehensive strategy to properly protect its submarine cable network from a range of threats, including from the subsea environment, inadvertent human activities and intentional attack.

Many federal and state government agencies have roles in this policy area, including MBC, the ADF, the Department of Home Affairs, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCSA), ACMA, DFAT,

ASD, and federal and state police. However, while these agencies are improving their cooperation, their respective roles and responsibilities for the protection of Australia's cables network are often overlapping and not clearly defined. There are currently no clear formal mechanisms for coordination among relevant agencies or binding understandings of which agencies have leading/supporting roles in respect of specific issues.

There is also a significant international element in protecting Australia's cables network. Submarine cables need to be protected along the entire length. By their nature, international submarine cables connecting Australia will cross numerous areas of national jurisdiction as well as the high seas. This factor makes it imperative for Australia to work with international partners to protect cables. There are also significant gaps in the international legal regime for the protection of submarine cables, making it very difficult to arrest and prosecute persons who disrupt or attack submarine cables outside Australian jurisdiction.

Sections 1 and 2 of this report establish the strategic and commercial context, examining Australia's dependence on submarine cables and the significant changes under way in the global cable industry – including the rise of the hyperscalers and the bifurcation of the industry along geopolitical lines. Section 3 provides the technical foundation necessary to understand the threats and vulnerabilities discussed later in the report, explaining how submarine cable systems work and how they relate to maritime jurisdictions. Section 4 examines Australia's current approach to governance and protection, identifying significant gaps in strategic guidance, legal frameworks, and the allocation of responsibilities among relevant agencies. Section 5 assesses the full range of threats facing submarine cables – environmental, human, and cyber – drawing on recent incidents in European and Indo-Pacific waters to illustrate the evolving threat environment. Sections 6, 7, and 8 turn to responses, examining how Australia can better protect its cables from disruption or attack, ensure timely access to repair capabilities, and work with industry and international partners to build resilience. Section 9 draws these threads together, making the case for a comprehensive national submarine cable strategy and setting out its key elements.

Connected & protected focuses on civilian telecommunications submarine cables. It does not address military seabed networks, which raise distinct operational and classification considerations.

In a deteriorating strategic environment marked by growing maritime instability, the strategic importance of Australia's submarine cables has never been more apparent – nor the consequences of their disruption more severe. Yet Australia's policy, regulatory frameworks, and capabilities have not kept pace with this evolving reality. This report provides a comprehensive assessment of Australia's submarine cable infrastructure – its strategic importance, the threats it faces, and the gaps in Australia's current policy, regulatory framework, and response capability. It makes a series of detailed recommendations for addressing these gaps, argues that Australia needs a comprehensive national submarine cable strategy, and sets out the key elements such a strategy should contain. It also identifies the significant economic opportunities that the shifting Indo-Pacific cable landscape presents, and how Australia can position itself to capture them.

Connected & protected was researched and written with funding support from the Australian Department of Defence, under its Strategic Policy Grant Program. All perspectives expressed in this report are those of the authors.

David Brewster

Samuel Bashfield

Jocelinn Kang

Mike Constable

Anthony Bergin

Canberra, Australia

August 2026

Australia's critical lines of communication

This section overviews the importance of submarine communications cables to Australia's economy, society, and security. It then discusses Australia's submarine cable networks, including existing and planned cables and cable landing stations, as well as Australia's growing role as an Indo-Pacific cable hub. It includes the following subsections:

1.1 The importance of submarine communications for Australia

1.2 Australia's submarine cable network

1.1 The importance of submarine communications for Australia

As an island nation with a globally integrated economy, Australia relies heavily on submarine cables for critical economic, governmental, security, and societal functions. Approximately 99 per cent of Australia's international data traffic transits submarine cables, making this seabed infrastructure the backbone of the nation's digital connectivity. These cables connecting Australia carry critical data including financial transactions worth trillions of dollars annually, government communications, cloud computing services, and the vast majority of internet traffic. For Australia, submarine cables are economic lifelines that underpin the functioning of modern society.

Major disruptions to submarine cables can have immediate and severe economic impacts, disrupting financial markets, halting international trade, and severing cloud-based services. Australia's financial sector, which processes billions of dollars in transactions daily, relies entirely on submarine cable connectivity to international markets. Government services, including defence communications and intelligence sharing with international partners, depend on secure cable infrastructure. Healthcare systems increasingly rely on international data flows for telemedicine and research collaboration.

The defence and national security dimensions of submarine cable reliance deserve particular emphasis. Australia's participation in the Five Eyes intelligence network, its defence relationships with the United States, United Kingdom, and other partners, and the operational requirements of the ADF all depend heavily on secure and reliable submarine cable connectivity. In a conflict, an adversary that successfully disrupted Australia's cable network would not only damage the civilian economy but would significantly degrade Australia's ability to communicate with allies, share intelligence, and coordinate military operations. Submarine cables are therefore not merely economic infrastructure – they are a critical enabler of Australia's defence and security partnerships.

According to a 2020 study by AustCyber,[2] the costs to the Australian economy of a one-week digital disruption due to a sophisticated cyber-attack would be A$5.9 billion (in 2025 dollars), and a four-week disruption would be A$35 billion (in 2025 dollars) and some 163,000 jobs. Given that a significant proportion of data systems depend on international connections, a prolonged disruption to Australia's submarine cable network could fundamentally compromise Australia's economic security.

Australia has few alternatives to its reliance on submarine cables, unlike some continental nations that may also have access to terrestrial fibre networks for international connectivity. Despite some improvements in satellite technology, satellite communications are unlikely to come close to matching the capacity, speed, or cost-effectiveness of submarine cables for the foreseeable future.

Year	2020	2021	2022	2023	2024	2020-24 CAGR
Gbps	15,205	20,546	29,062	37,252	49,090	34%

Figure 1: International bandwidth usage for Australia (Gbps). Source TeleGeography.

Australia is growing ever more reliant on submarine cables for international communications. As shown in Figure 1, Australia's demand for submarine cable capacity is growing strongly. Between 2020 and 2024, Australia's international bandwidth demand grew at a compound annual growth rate (CAGR) of 34 per cent, increasing from 15,205 Gbps to 49,090 Gbps. This level of growth reflects the increasing digitisation of the Australian economy and the growing data intensity of everyday activities. Cloud computing has moved from niche technology to default infrastructure for business operations, with Australian organisations storing data and running applications on servers across the globe. Remote work, now embedded in Australian work culture, requires constant high-bandwidth international connectivity.

The emergence of artificial intelligence is creating substantial new bandwidth demands. AI systems require access to vast datasets for training, often necessitating the transfer of petabytes of data across international networks. Australian researchers, businesses, and government agencies increasingly rely on AI services hosted in overseas data centres. As AI becomes integrated into medical diagnostics, autonomous vehicles, and government service delivery, Australia's dependence on reliable, high-capacity submarine cable infrastructure will only deepen. The data volumes involved in AI applications dwarf those of previous internet eras.

Data centres serve as critical junction points where submarine cables meet terrestrial infrastructure. Australia's major data centre hubs in Sydney, Perth, Melbourne, and increasingly Darwin, house the equipment that interfaces between submarine cable systems and domestic networks. Major international technology companies, including hyperscalers such as Google, Amazon, Microsoft, and Meta, are investing heavily in new cable connections and/or Australian data centre infrastructure. These investments reflect Australia's emerging role as a regional data hub, where international traffic can be processed and routed across the Indo-Pacific. The security and resilience of these data centres and their connections to submarine cable infrastructure are matters of national strategic importance.

1.2 Australia's submarine cable network

International and domestic cables

Australia is served by 16 operational international submarine cables that connect the continent to Asia, the Americas, the Middle East, and the Pacific Islands. Domestic cables also connect several major capital cities as well as offshore connections to Tasmania, Kangaroo Island, and Groote Eylandt (see Figures 2 and 3).

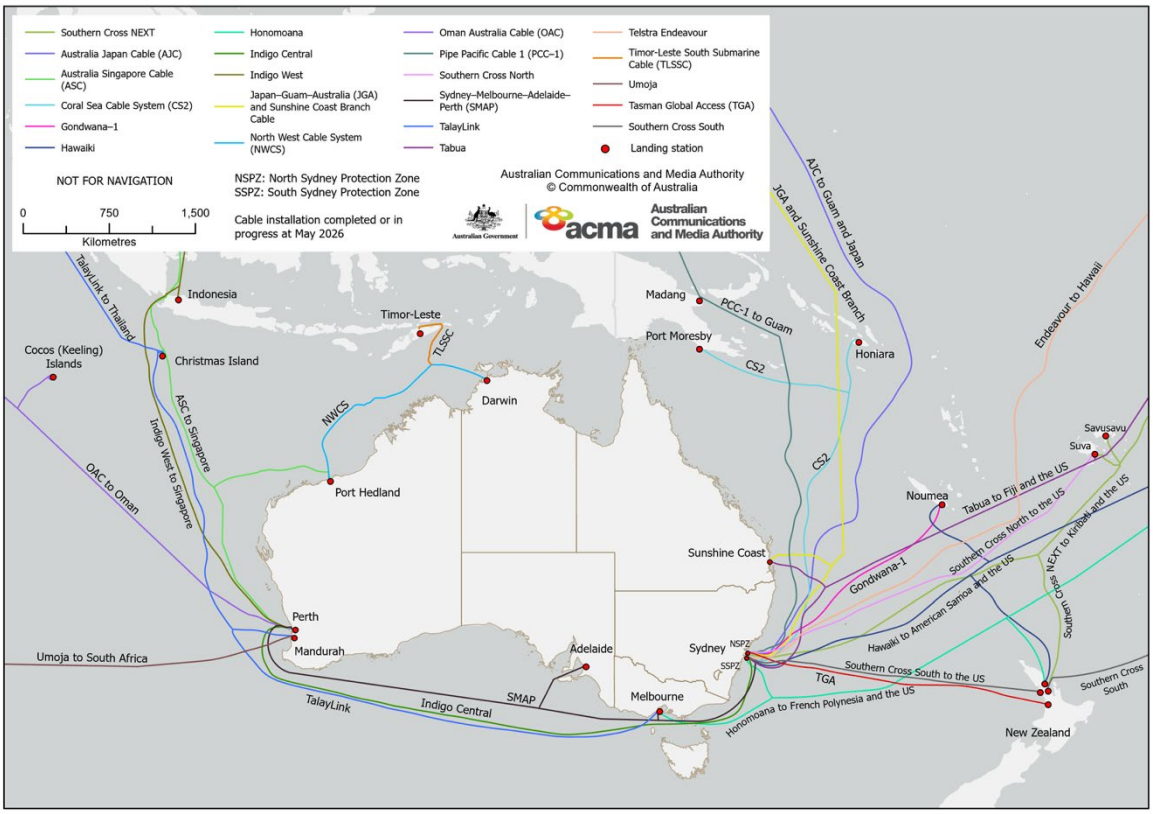


Figure 2: Map of in-service and planned international submarine cables connecting Australia as at May 2026. Source: https://www.acma.gov.au/international-submarine-cables-landing-australia.

As can be seen, most of Australia's international cable connections are trans-Pacific, linking Australia with New Zealand, the Pacific Islands and the US. There are a smaller, but growing, number of installed and planned connections across the Indian Ocean. These mostly connect Australia with Southeast Asia and Europe via Singapore. The Oman Australia Cable, completed in 2022, provides Australia's first direct connection to the Middle East, diversifying routes that previously required transit through Southeast Asia.

Submarine network name	Current owner(s)	RFS year	Length (km)
Timor-Leste South Submarine Cable	Government of Timor-Leste	2025	607
Kangaroo Island 2	SA Power Networks	2024	15
Darwin-Jakarta-Singapore Cable	Vocus Communications	2023	7,700
Oman Australia Cable	SUBCO	2022	11,000
Southern Cross NEXT	Southern Cross Cable Network	2022	13,700
Japan-Guam-Australia South	Australia's Academic and Research Network (AARNet), Google, Light-storm Telecom	2020	7,081
Coral Sea Cable System (CS^2)	PNG DataCo Limited, Solomon Island Submarine Cable Company	2020	4,700
INDIGO-Central	AARNet, Google, Indosat Ooredoo, Singtel Optus, Superloop	2019	4,850
INDIGO-West	AARNet, Google, Indosat Ooredoo, Singtel, Superloop, Telstra	2019	4,600
Hawaiki	BW Digital	2018	14,000
Australia-Singapore Cable	Vocus Communications	2018	4,600
Tasman Global Access Cable	One NZ, Spark New Zealand, Telstra	2017	2,288
North-West Cable System	Vocus Communications	2016	2,100
Groote Eylandt	Telstra	2011	95
PIPE Pacific Cable-1	Vocus Communications	2009	6,900
Telstra Endeavour	Telstra	2008	9,125
Gondwana-1	OPT	2008	2,151
Basslink	Basslink Telecoms	2005	298
Bass Strait-2	Telstra	2003	239
Australia-Japan Cable	AT&T, NTT, Softbank, Telstra, Verizon	2001	12,700
Southern Cross Cable Network	Southern Cross Cable Network	2000	30,500
Bass Strait-1	Telstra	1995	241

Figure 3: In-service international and domestic submarine cables connecting Australia, as at January 2026. Source: TeleGeography and industry input.

The international cables serving Australia reflect different ownership models and purposes. Traditional telecommunications carriers including Telstra, Singtel Optus, and Vocus operate several systems, while newer cable owner/operators reflect the growing dominance of technology companies in submarine infrastructure. For example, the INDIGO cable system, which connects Australia to Singapore via Indonesia, is jointly owned by a consortium including Australia's Academic and Research Network (AARNet), Google, and major telecommunications providers. Based on publicly available information, none of the cable systems that connect with Australia have Chinese ownership or operation or use Chinese equipment.

Australia's newest international cables reflect both the increasing data demands of the digital economy and evolving strategic considerations. The Darwin-Jakarta-Singapore Cable (part of the North West Cable System), which became operational in 2023, provides northern Australia with direct connectivity to Southeast Asia, reducing reliance on southern routes. The Japan-Guam-Australia South cable enhances connectivity with key Indo-Pacific partners. The Australia-Singapore Cable and INDIGO cables provide critical links to Singapore, one of Asia's major digital hubs, though these routes transit through geopolitically sensitive waters, including the Sunda Strait.

Among the operators active in Australia's cable network, it is worth noting the growing significance of Australian companies. Telstra, Vocus Communications, and SUBCO are Australian-based with multiple cable systems and landing stations. Their ownership profile represents a different strategic consideration from cables operated by foreign telecommunications consortia or hyperscalers. Australian-owned operators are more directly subject to Australian law and government direction and may be more responsive to national priorities in a crisis, with already established relationships with Canberra.

In addition to international cables, Australia maintains several domestic submarine telecommunication cables that provide critical connectivity to offshore islands and territories. These include three cables linking Tasmania to the Victorian mainland (Bass Strait-1, Bass Strait-2, and Basslink), as well as cables serving Kangaroo Island off South Australia and Groote Eylandt in the Northern Territory. Tasmania's dependence on submarine cables for telecommunications highlights the critical nature of this infrastructure for isolated regions. The Sydney-Melbourne-Adelaide-Perth cable, currently under construction with expected completion in 2026, will provide high-capacity backbone connectivity along Australia's southern coast. While shorter in length than international systems, these domestic cables are essential for ensuring national network resilience and providing reliable connectivity to island communities and infrastructure.

Several major international submarine cable projects are currently under construction or planned, which would significantly expand Australia's international connectivity (see Figure 4). Google is investing heavily in cables connecting Australia, including the Tabua cable (expected 2026), Honomoana (2026), and Umoja (2027) among others, reflecting the hyperscalers' growing role in submarine infrastructure. The planned 10,000-kilometre Hawaiki Nui 1 cable will enhance trans-Pacific connectivity to Southeast Asia. These upcoming cables, if deployed, would greatly expand Australia's international bandwidth capacity within the next few years, accommodating the strong growth in data demand driven by cloud computing, AI, and increasing digitisation.

Submarine network name	Owner	RFS year	Length (km)
Project Waterworth	Meta	n.d.	50,000
APX East[3]	SUBCO	2028	
SX Tasman Express (SX-TX)	Southern Cross Cable Network	2028	2,276
Dhivaru	Google	2028	
Tasman Ring Network	Datagrid New Zealand	2027	6,000
Bosun	Google	2027	
TalayLink	Google	2027	
Umoja	Google	2027	
Hawaiki Nui 1	BW Digital	2027	10,000
Tabua	Google	2026	
Honomoana	Google	2026	15,215
Sydney-Melbourne-Adelaide-Perth	SUBCO	2026	5,000

Figure 4: Planned cables connecting Australia, as at January 2026. Source: TeleGeography and public reports.

Australia is assuming an increasingly important role as a data conduit between the Americas and Asia, the Middle East, and Europe. The 'Great Southern Route', which connects the Pacific and Indian oceans, transiting south of the Australian continent, is increasingly being used to bypass Southeast Asian waters. This route offers advantages in terms of geographic diversity, avoiding the congested and geopolitically sensitive South China Sea and Malacca Strait. Large US hyperscalers – particularly Google, but also Meta – are investing significant amounts in submarine cable networks in the Pacific and Indian oceans that connect Australia, acknowledging the continent's strategic position as a stable, technologically advanced hub in the Indo-Pacific. These hyperscaler investments represent a fundamental shift in the submarine cable industry, with technology companies now driving infrastructure development based on respective data centre strategies, rather than relying on traditional telecommunications carriers.

Australia also has significant interests in connecting the Australian Antarctic Territory and acting as a hub to connect with Antarctic research stations operated by other countries. Preliminary consideration has also been given to developing a submarine cable between Australia and the Antarctic to service the large data needs of Antarctic scientific research stations and potentially also operate as an environmental monitoring tool.[4] This is discussed further below.

An Antarctic submarine cable for Australia?

Dr Tony Press, University of Tasmania

Antarctica remains the only continent not connected to the rest of the world by submarine telecommunications cable. The use of satellite communications to transmit large amounts of scientific data is becoming increasingly problematic due to significant bandwidth constraints and power needs.

Australia has significant interests in Antarctica, claiming some 42 per cent of the continent as Australian territory, as well as maintaining three research stations on the continent and another on sub-Antarctic Macquarie Island. In recent years, the Australian Government has made considerable investments to consolidate its presence, including acquiring a state-of-the-art Antarctic icebreaker, RSV *Nuyina,* investing in upgrading Hobart-based Antarctic logistic facilities, and maintaining and operating the Wilkins aerodrome near Casey Station.

In 2021, an Australian parliamentary inquiry considered the question of developing communications infrastructure with Antarctica.[5] The Australian Antarctic Division submitted that Australia should undertake an engineering study to determine the feasibility of connecting one or more of our Antarctic stations via submarine fibre cable, and framed the submission in terms of both addressing current telecommunications constraints, and Australian leadership in Antarctic affairs.[6] The Australian Bureau of Meteorology also recommended that the government should investigate the feasibility of establishing an intercontinental and intracontinental fibre optic cable technology and infrastructure to permanent Antarctic research stations.[7]

Currently, there are two active proposals to lay fibre optic cables to Antarctica: one from the US led by the National Science Foundation (NSF), and a Chilean proposal led by the Undersecretariat of Telecommunications (SUBTEL). The Chilean proposal would connect Puerto Williams in Chile to King George Island in Antarctica, with a feasibility study due to be completed in 2026.[8] The US proposal could possibly provide a direct benefit to Australia for telecommunications, scientific data transfer, and marine research. Its Science Monitoring and Reliable Telecommunications (SMART) cable would connect McMurdo station with either Sydney or Invercargill in New Zealand. Either route would require additional costs to address environmental issues in the Antarctic, such as the presence of icebergs. Both proposals are centred on increasing telecommunications capacity and capability to and from Antarctica. The cables would also carry *in situ* scientific sensors for a broad range of scientific research purposes.[9]

McMurdo Station is the largest Antarctic base and is the key logistics hub for US Antarctic re-supply, field operations, and connection to the US Scott Polar Research Station at the South Pole. The US SMART proposal would have benefit to Australia, not only because it would allow for the US to transmit large volumes of data in real time from Antarctica, but also because it could potentially allow branch telecommunications cables to be laid to subantarctic Macquarie Island, and possibly further afield to one or more of Australia's Antarctic research stations. Having fibre-optic cable connectivity to Macquarie would enhance the capabilities of Australian government agencies with facilities on Macquarie Island for:

- the Bureau of Meteorology, which has globally significant weather and climate facilities on the island
- the Australian Radiation Protection and Nuclear Safety Agency, which operates a facility under the Comprehensive Nuclear Test Ban Treaty
- Geosciences Australia, which operates a geomagnetic observatory of space weather, along with seismic stations for earthquake monitoring, nuclear test monitoring, and other observations; and
- the Australian Antarctic Division, which operates, supplies, and supports the station and the scientific research programs undertaken there.

Using the cable to carry diverse scientific instrumentation would also open up new marine science capacity and capabilities in the data-poor Southern Ocean. The NSF issued a Request for Information in late 2024 for the SMART proposal.[10] There has not been any update from the NSF on the proposal since then.

The Australian Government should carefully consider participating in the US SMART proposal as it has the capability to benefit Australian Antarctic and Southern Ocean science. The SMART proposal also provides the potential platform for connections to Macquarie Island, and to other parts of Antarctica.

The expansion and diversification of Australia's submarine cable network is both a resilience imperative and an economic opportunity. As Indo-Pacific cable routes are redrawn away from geopolitically sensitive chokepoints, Australia is well-positioned to attract new investment as a stable, trusted hub connecting the Pacific and Indian oceans. These new cables significantly enhance the resilience of Australia's communications, as well as enhance the digital connectivity of Australia's Indo-Pacific partners. Realising this opportunity – while managing new strategic considerations around route diversity, ownership models, and the concentration of landing points – requires a coherent national approach to submarine cable policy.

Cable landing stations

Australia's cables currently land at 17 cable landing stations (CLSs) distributed across the country, with Sydney and Perth hosting most of the country's international cable connections. Additional landing stations, including those that service domestic cables, are located in Darwin, the Victorian coast, the Sunshine Coast, and various regional locations including Port Hedland, Wurrumiyanga, and multiple sites in Tasmania (see Figure 5). It is likely that new cable landing stations will be developed to service new cable connections.

Location	Station name	Operator	No of cables	Cable names
Adelaide	SUBCO CLS	SUBCO	1	Sydney-Melbourne-Adelaide-Perth
Alexandria, Sydney	Singtel Optus CLS	Singtel Optus	3	INDIGO-Central, Southern Cross NEXT, Southern Cross Cable Network
Boat Harbour, Tasmania	Telstra CLS	Telstra	1	Bass Strait-1
Brisbane	Brisbane CLS		1	Hawaiki Nui 1
Brookvale, Sydney	Singtel Optus CLS	Singtel Optus	3	Gondwana-1, Southern Cross Cable Network, Japan-Guam-Australia South
Darwin	NEXTDC CLS	NEXTDC	1	North-West Cable System
Four Mile Bluff, Tasmania	Basslink Telecoms CLS	Basslink Telecoms	1	Basslink
Inverloch, Victoria	Telstra CLS	Telstra	1	Bass Strait-2
Maroochydore, Queensland	Sunshine Coast CLS	NEXTDC	1	Japan-Guam-Australia South
McGaurans Beach, Victoria	Basslink Telecoms CLS	Basslink Telecoms	1	Basslink
Melbourne	SUBCO CLS	SUBCO	2	TalayLink, Sydney-Melbourne-Adelaide-Perth
Oxford Falls, Sydney	Telstra CLS	Telstra	2	Tasman Global Access Cable, Australia-Japan Cable
Paddington, Sydney	Telstra CLS	Telstra	3	Telstra Endeavour, Coral Sea Cable System, Australia-Japan Cable
Perth	Equinix CLS	Equinix	2	Sydney-Melbourne-Adelaide-Perth, Australia-Singapore Cable
Port Hedland, Western Australia	NEXTDC CLS	NEXTDC	2	North-West Cable System, Darwin-Jakarta-Singapore Cable
Sandy Point, Victoria	Telstra CLS	Telstra	1	Bass Strait-1

Location	Station name	Operator	No of cables	Cable names
Stanley, Tasmania	Telstra CLS	Telstra	1	Bass Strait-2
Sydney	Equinix CLS	Equinix	1	Tabua
Sydney	Equinix SY4 & SY5	Equinix	2	Sydney-Melbourne-Adelaide-Perth, Hawaiki
Sydney	TPG Corporation (incl. iiNet and Internode) CLS	Vocus	1	PIPE Pacific Cable-1
Wurrumiyanga, Northern Territory	Wurrumiyanga CLS	Vocus	1	North-West Cable System

Figure 5: Australia's Cable Landing Stations as at January 2026. Source: TeleGeography.

This dispersed network of landing stations provides a degree of geographic redundancy, though the concentration of capacity in Sydney and Perth means these two cities remain critical nodes in Australia's digital infrastructure. The rapid expansion of Australia's cable network, and its growing role as an Indo-Pacific hub, makes the need for a coherent national approach to cable policy and protection even more urgent.

The changing dynamics of the submarine cable industry

This section discusses how the international submarine cable industry has evolved over the past decade, including in response to geopolitical developments, the growth of a handful of US-based technology companies as major data users, the broadening submarine cable investor base, and the impact of data centres and AI. It then considers the potential consequences of these developments for Australia.[11] This section contains the following subsections:

2.1 Bifurcation of the cables equipment and services industry

2.2 The rise of the hyperscalers

2.3 The impact of data centres and AI

2.4 Potential impact of new technological developments

2.5 Consequences for Australia

Australia's approach to governing its network of international submarine cables is fundamentally affected by the nature of the industry. In Australia and elsewhere, international submarine cables are predominantly owned and operated by private companies, and new development is being increasingly dominated by the hyperscaler cloud and content providers.

Until the 1980s and 1990s, the great majority of international communications cables were owned and operated by major, generally state-owned, telecommunications companies, often working in international consortiums. Through the 1990s, the ownership structure of the industry changed with the privatisation of many state-owned telecommunications companies, regulatory liberalisation, and the entry of new specialist private operators that built new cable systems, often on a speculative basis. Over the last decade or so, the industry has become increasingly dominated by the hyperscalers, which have become the dominant users of international bandwidth and are pursuing backward integration strategies to own and control connectivity infrastructure that services their data centres and cloud-based applications.

In recent years, the international cables industry has been significantly affected by geopolitical tensions between China and the US after the US imposed export sanctions on Chinese telecom equipment makers such as Huawei and ZTT. This was followed by the US 'Trusted Network' initiative, which led to a bifurcation of the industry between Chinese and non-Chinese equipment suppliers and service providers. Security concerns regarding China, Russia, and others are also influencing the re-routing of cables outside of areas where there are particular security concerns, including in the South China Sea.

Data centres are increasingly influencing the investment and routing of new cables. Whereas historically cables were laid to optimise connections between end-users (for example, to connect major cities in different countries), most of the traffic now flows between data centres. Data centre connectivity will accelerate due to the escalating influence of AI on bandwidth demand between data centres. AI labs developing foundational (large language) models, such as Anthropic and OpenAI, are now actively seeking direct international bandwidth, as are chip architects such as Nvidia to expand its 'GPU as a service' cloud applications.

The private nature of the industry, including in ownership, operation, component supply, and servicing, has several policy consequences for Australia. Australia's current international cables network now has no more than around four to five major players, including companies such as Telstra (the legacy telecoms provider), Vocus, and SUBCO, which are being joined by the US-based hyperscalers. The configuration, landing location, and design capacity of cables will be determined by private investment decisions, often foreign based, with little input from government. Similarly, the Australian Government has little input into maintenance of this vital infrastructure. While private companies may want their invest-

ments protected by government legislation and action, these firms are also likely to resist government 'interference' in their operations.

2.1 Bifurcation of the cables equipment and services industry

The international cable industry features a concentrated supply chain dominated by a small number of players in cable design, engineering, equipment manufacturing, and construction services. These cable system suppliers are led by the so-called 'big four' companies: the US-based SubCom, France's ASN, Japan's NEC, and China's HMN Technologies. China's HMN Technologies has a smaller market share, driven in part by geopolitical influences and the 'Trusted Network' initiative. Figure 6 shows the percentages of cables delivered by major suppliers in the period 2010–24 against 2025–27.

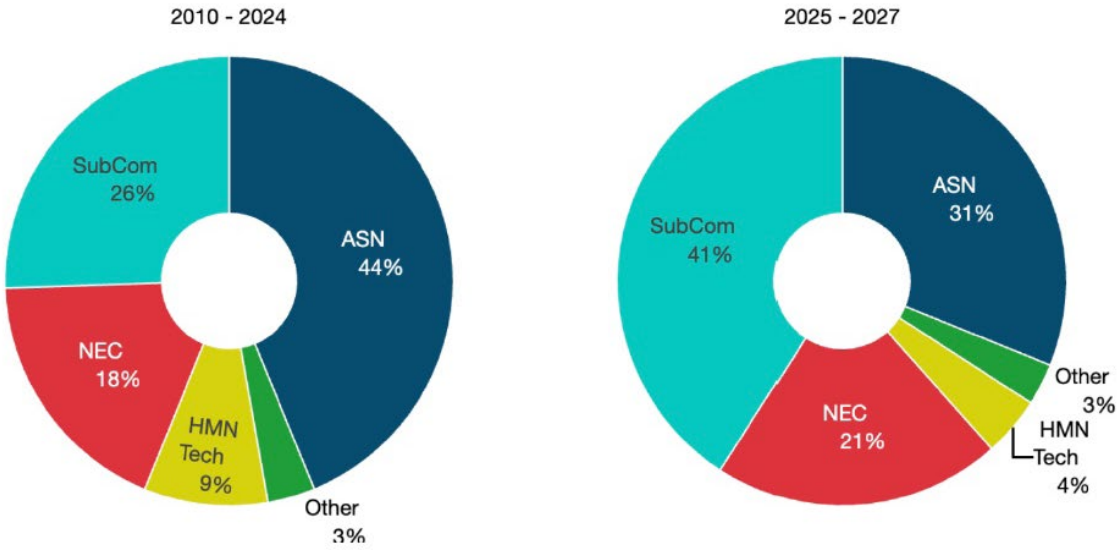


Figure 6: Percentage share of cables by supplier in selected years. Source: Stronge, TeleGeography. Pacific Telecommunications Council presentation, 2026.

Other parts of the international cable ecosystem, such as vessel providers that support cable laying, and maintenance and repair services, are also characterised by a small number of players. These include UK-headquartered, Singapore-owned Global Marine Group, France's Orange Marine, Malaysia-based, Malaysia- and US-owned Optic Marine Services, Singapore-based Asean Cableship, Japanese operators NTT and KDDI, and China's SB Submarine Systems.

Rising geopolitical tensions in recent years have led to important changes to the industry. Over the last several years the structural division of the industry between Chinese and Western companies that build, operate, supply, and service cable systems is underpinned by a clear shift from the 'Trusted Network' to a 'Trusted Supply Chain' initiative. This has largely been driven by the US, Australia, and other countries that are concerned about reliance on Chinese equipment, operators, and service suppliers.

The growing division between Chinese and other global suppliers and operators is shown in Figure 7.

	Chinese companies	Global rivals
Main investors	China Telecom, China Mobile, China Unicom	Google (US), Amazon (US), Meta (US), Microsoft (US)
Cable system suppliers (equipment suppliers and cable ship operators)	HMN Technologies, FiberHome	SubCom (US), Alcatel Submarine Networks (France), NEC (Japan), Xtera (UK)
Fibre-optic cable manufacturers	Hengtong, FiberHome, Yangtze Optical Fibre and Cable, Jiangsu Zhongtian Technology	Corning (US), Nexans (France), NEC (Japan), Furukawa Electric (Japan), Prysmian (Italy)
Optical components, chips	Wuhan Fisilink Microelectronics Technology, Huawei Technologies, Zhongji InnoLight, Accelink Technologies	Broadcom (US), Coherent (US), Sumitomo Electric Industries (Japan)
Repeaters	HMN Tech, FiberHome	NEC (Japan), SubCom (US), ASN (France), Xtera (UK)
Cable ship operators	FiberHome Marine, China Telecom, S.B. Submarine Systems	Global Marine Group (UK), Asean Cableship (Singapore), OMS (Malaysia), Orange Marine (France), NTT WEM, KDDI (Japan), IT Telecom (Canada), [SubCom (US)]
Data centre, servers	Huawei, Inspur, Lenovo	Google (US), Meta (US), Amazon (US)[12]

Figure 7: Bifurcation of the submarine cables industry. Source: Cheng Ting-Fang, Lauly Li, Tsubasa Suruga, Shunsuke Tabeta, 'China's subsea cable drive defies US sanctions', Nikkei Asia, 26 June 2024, as amended by authors.

Through its 'Trusted Network' policy, the US Government has sought to discourage participation by China, Russia, and selected other countries in cables connecting with the US, as well as cables elsewhere in the world. This policy initially focused on system suppliers that design, manufacture, and deploy cables and the provision of telecom equipment, but is now extending the policy to ownership interests in cables – including indefeasible right of use (IRU) owners – and the companies that provide maintenance services.[13]

In 2021, for example, in order to secure US landing rights for their proposed trans-Pacific Ocean Pacific Light Cable Network, the US Government forced Google and Meta to sign an agreement to drop a proposed Hong Kong landing site and exclude a Chinese investor. Instead, they were required to "pursue diversification of interconnection points in Asia, including but not limited to Indonesia, Philippines, Thailand, Singapore and Vietnam".[14] In practice, the US Government has also informally extended its trusted supplier policy beyond cables that directly link with the US to cables located elsewhere in the world, including through diplomatic pressure as well as offers of training grants and export finance to cable operators.[15]

The US Government also uses hyperscalers such as Google, Meta, Microsoft, and Amazon (all based in the US), as major points of leverage in support of its 'Trusted Network' policies. Under pressure from the US Government, the hyperscalers are now declining to take capacity on new Chinese-built cables, including cables that do not directly connect with the US (although in practice on occasion they may acquire capacity on such cables through third parties). Given their share of the data transmission market, the threat that hyperscalers will re-route traffic to avoid Chinese-built cables is a highly potent one for many cable operators in making investment decisions.

Through these tools, in 2023 the US Government was able to successfully exclude Chinese equipment and service providers (and, as a consequence, also Chinese equity investors) from participating in the South East Asia – Middle East – Western Europe 6 (SEA-ME-WE 6) cable that will connect Southeast Asia, the Middle East, and Western Europe, despite their bid being significantly cheaper than US suppliers.[16] The US Government is also placing pressure on Vietnam to disallow China's HMN Technologies from supplying equipment and services for the 10 new submarine cables that Vietnam plans to build by 2030.[17]

Although US hostility towards Chinese involvement in submarine cables has no doubt heightened in recent years, concerns have existed for decades. As far back as 2002, the US also blocked the planned acquisition of Global Crossing, which had major cable investments around the world, by a consortium that included Hong Kong-based Hutchinson Telecommunications as well as insisting that the company should be subject to significant security measures.[18] US policy towards the global submarine cable industry is coordinated by a government committee known as 'Team Telecom' comprising representatives from the departments of Justice, Defense, and Homeland Security, and several other agencies.

For its part, the Australian Government has taken a leading role in supporting and subsidising new cable systems in the Pacific Ocean to provide more attractive alternatives to proposals by Chinese companies to build new cable systems. Beginning in 2019, the Australian Government contributed two thirds of funding for the Coral Sea Cable System connecting Australia with Solomon Islands and PNG to stymie a proposed cable to be built by Huawei Marine Networks (now HMN Technologies). Through the AIFFP, the Australian Government has financed projects relating to submarine cables in Timor-Leste, Palau, Tonga, and Tuvalu, amongst others.[19] Most recently, Australia invested in a Google-sponsored cable connecting with several points in PNG.[20]

These developments mean that new cables being developed by the hyperscalers will not use Chinese equipment or service suppliers (although Chinese-manufactured components may be used within optical or electronic sub-assemblies).[21] Other prospective investors in new cables are also increasingly being forced to choose between their project being classified as a 'non-trusted' cable that incorporates Chinese-supplied equipment and services or as a 'trusted' cable with non-Chinese equipment/services. There is no publicly available information on the extent to which existing cables connecting with Australia incorporate components from 'non-trusted' suppliers.

2.2 The rise of the hyperscalers

Another major change to the cables industry in recent times has been the rise of the hyperscalers, who are now building dedicated cables around the world to service their respective data transfer needs, particularly between regional data centres. Google, Meta, Microsoft, and Amazon reportedly account for some 71 per cent of all used international capacity,[22] while other tech companies such as Apple, Netflix, Alibaba, ByteDance, and Akamai reportedly use much of the remaining capacity.[23]

The hyperscalers' massive bandwidth demand, combined with their respective financial resources and market power, are fundamentally altering the industry. From being significant co-investors in several cables as far back as 2010, in the past few years there has been a shift from a co-investment model to a sole investment model in many cables, particularly in the case of Google and Meta. Their position as major bandwidth users and massive balance sheet resources give the hyperscalers considerable advantages over traditional investors, who may scramble to put together investment models that require external financing.

According to Kang and Jacob, hyperscalers were key investors in some 23 per cent of cable systems that commenced operations between 2019 and 2023. According to another report, as of 2020, Google, Microsoft, Facebook, and Amazon together owned or leased nearly half of all global undersea bandwidth.[24] The current proportion of hyperscaler investment in cables is likely considerably higher and expected to accelerate in coming years.

Figure 8 shows the relative proportions of planned investment by hyperscalers (alone and in consortia) and others over the period 2025–29, by major region.

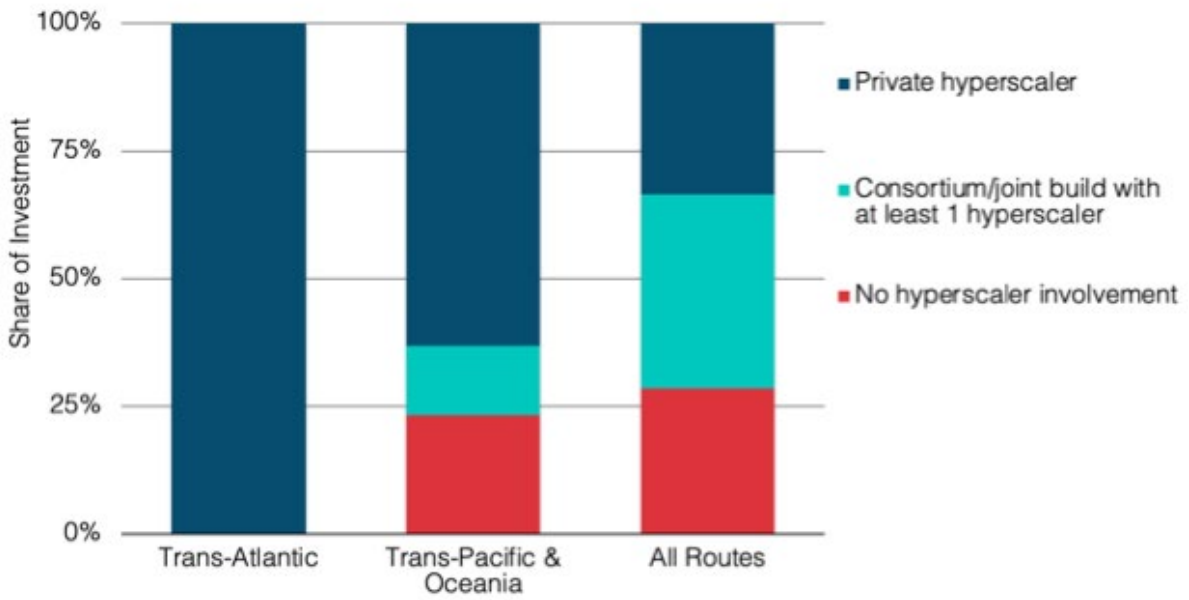


Figure 8: New cable investment by region 2025-2029. Source: Boudreau, Strong, Hjembo, TeleGeography Workshop, Pacific Telecommunications Council, 2026.

The growing domination of the hyperscalers has several consequences. For one thing, their significant investment in new cables boosts the submarine cable network's resilience by adding route redundancy and geographic diversity. In addition, they hold considerable market power and leverage across the industry supply chain, including cable system supply and maintenance and repair services. Hyperscaler investment has also accelerated technological innovation that has significantly expanded the total capacity of cable systems.

The scale of US-based hyperscalers' ownership and control over a significant portion of the global cable network, coupled with their explosion in data centre investment, is transforming the digital infrastructure landscape. This investment and ownership profile has the potential to create a digital infrastructure dependency across data connectivity, data storage and data compute elements. This means that a potential disruption (for example through cyber-attack) of one or more of the hyperscalers' digital infrastructure assets, could have widespread consequences for a large portion of international connectivity, data transmission and cloud-based digital services. The impact of such an event may be catastrophic.

The dominance of US-based hyperscalers (and/or other US-based technology companies – see below) could also potentially create concerns for Australia related to sovereign control. This dynamic would have implications for Australia's ability to maintain vital international communications. Further, it is not just the US-based hyperscalers that are changing the investment landscape. Major Chinese communications companies such as China Mobile, China Telecom and China Unicom are making significant investments in new cables, whether alone or as part of regional consortia, which may have significant security implications for Australia.

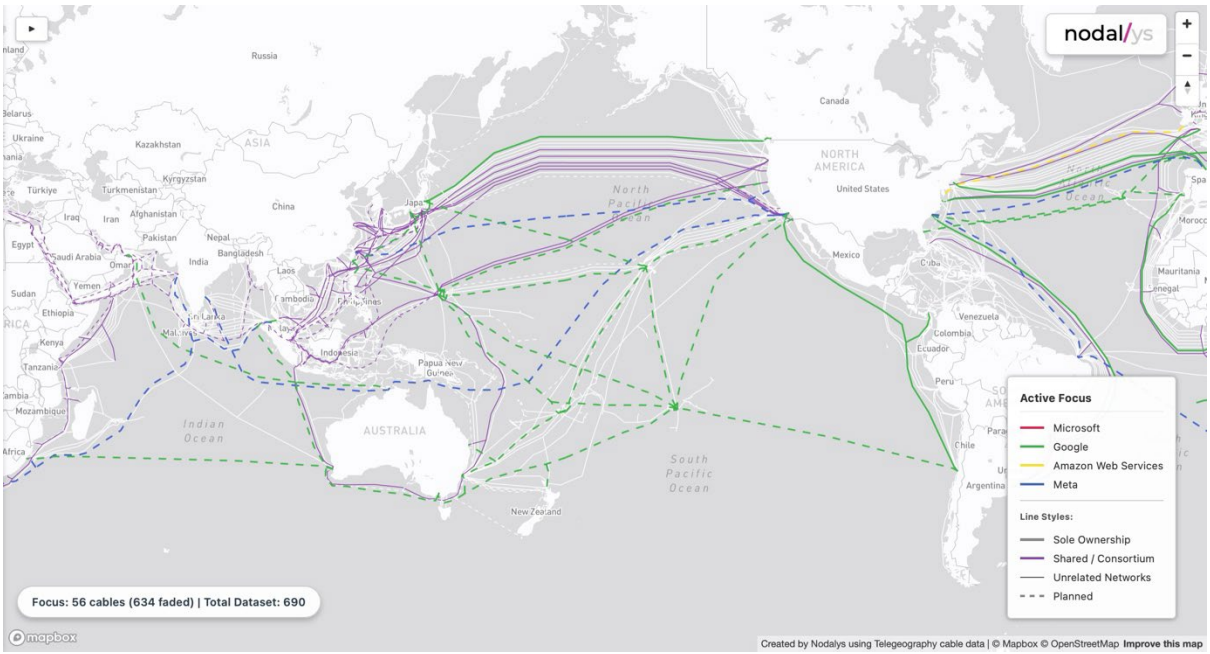


Figure 9: Hyperscaler-owned or planned cables. Source: Nodalys.

2.3 The impact of data centres and AI

As previously noted, new cables were originally laid to optimise connections between major population centres in different countries. However, the majority of traffic that flows between data centres is no longer primarily generated by humans (for example, a person searching the internet or uploading video content). Instead, it is machine-generated by social media companies and others continuously updating information between servers in data centres located in data centre clusters or hubs. Other factors, such as data sovereignty regulations adopted by many countries – including Australia – require some user data to be stored locally, adding to the demand for data centre connectivity. Social media, 5G mobile networks, the Internet of Things (IoT), self-driving vehicles, and numerous other data-driven applications, combined with the accelerating adoption of AI services, all require as much data to be stored near end users, further driving demand for data centre connectivity.

The synergies between data centre location and cable connectivity means that investment decisions concerning the location of data centres have an influence on cable landing locations, particularly where data centres are located in coastal regions. Other infrastructure utilities, notably the access to reliable, renewable energy also have significant influence over data centre location, as does political and economic stability, and favourable investment policies of host states. The confluence of international cable connectivity, data centres, and access to renewable energy sources is illustrated by proposals to develop large-scale data centre infrastructure in Australia's Northern Territory. This development will be linked to renewable energy projects such as SunCable and international connectivity via Google's Australia Connect cable initiative, which will connect Darwin and Australia's west coast to Christmas Island and onward to Asia.

While this space is currently being dominated by the hyperscalers (principally Google and Meta, as well as Amazon and Microsoft) the AI revolution could also lead key AI companies (e.g. Anthropic, Nvidia or others) to become major investors in submarine cable connectivity if they determine that such infrastructure is in their respective interests to own and control.

Government policy can have a significant impact on these decisions. For example, between 2019–22, Singapore imposed a moratorium on the development of new data centres because of concerns about corresponding high energy consumption. Although data centres are now being built under a 'Green Data Centre Roadmap', there were fears that restrictions on data centres could affect Singapore's role as a regional cable hub if hyperscalers decide to by-pass Singapore for new investments. It is notable that data centre hubs have also grown on the Indonesian island of Batam and in the Malaysian state of Johor, both locations in close proximity to Singapore that have ample connectivity to Singapore by submarine cables and terrestrial fibre networks.

2.4 Potential impact of new technological developments

Submarine and terrestrial fibre optic cables currently provide most of the capacity for international data transmission. The use of fibre-optic cables is helped by technological developments that are contributing to major increases in efficiency and bandwidth. Advances in optical multiplexing technology can significantly increase the amount of data that can be transmitted on new, and upgraded, fibre-optic cables.

Alternative technologies such as data transmission by satellite are far more expensive than fibre optic cables and are highly constrained by radio broadcast bandwidth, generally only allowing transmission at rates of several gigabits per second (although Starlink can reportedly deliver up to 20 Gbps per satellite).[25] Many satellite configurations (particularly satellites in geosynchronous orbit) also add considerable latency to data transmission. Satellites therefore currently provide only a partial and minor complementary alternative to fibre-optic cable data transmission and are largely used in remote regions or in other circumstances where cable transmission may not be available.

Industry analysts also point out that the comparative cost of bandwidth on submarine cables is a fraction of the cost on satellite systems. Estimates suggest the differential between bandwidth unit costs is approximately 2,800 per cent higher on satellite systems.

However, this may not always be the case. Optical communication technology using lasers has the potential to provide satellites with much greater bandwidth by providing up to 1,000 times the data rates currently available through radio transmission. The deployment of optical communications on satellites is under development. The first operational optical ground station network in the Southern Hemisphere was opened in Western Australia in 2025, with further ground stations planned for other Australian states and territories.[26] Overall, these developments may eventually give satellites the potential to compete with fibre-optic data transmission, at least under certain circumstances.

2.5 Consequences for Australia

These developments will have five significant consequences for Australia. First, hyperscalers' investments in new cables have the potential to enhance the geographic diversity and redundancy in Australia's cable connections, including through promoting Australia as a new pathway for cable connectivity between the Indian and Pacific oceans. The use of Australia as a transregional hub may allow new cables to avoid locations that are perceived to be geopolitically risky (e.g. the South China Sea or Malacca Strait) or waters where local regulatory regimes are perceived as unfavourable or unduly challenging to investors (e.g. Indonesia or Malaysia).

Second, Australia's potential as a trans-Indo-Pacific cable hub is further enhanced by its preferred location for data centres in providing a politically/economically stable environment with access to reliable, relatively cheap energy, including renewables.

Third, the massive level of investments in new cables by the hyperscalers, particularly Google, along with the progressive decommissioning of existing cables as they reach the end of service life, could give Google and other US-based hyperscalers a high degree of dominance over Australia's international cable network. This may significantly undermine the Australian Government's ultimate control over the country's international communications.

Fourth, emerging partnership models between hyperscalers and Australian-owned operators offer a potentially productive middle path between full hyperscaler dominance and traditional carrier-led investment. Under such models, a US-based hyperscaler co-funds cable construction while an Australian-owned operator provides landing infrastructure, operations, and domestic backhaul – with state and local government involvement – in landing locations. This structure can simultaneously deliver hyperscaler capital and route diversity while preserving a degree of Australian ownership and operational control. The Australian Government should consider how policy settings can encourage and build on this partnership model.

Fifth, the investments by Chinese state-owned carriers in regional cable systems raise a distinct risk of economic coercion. A state such as China that exercises control over cable infrastructure, whether through ownership of cable operators, landing stations, or the territory through which cables transit, could throttle, condition, or deny access to data traffic as an instrument of economic or political leverage. Countries with limited redundancy or few alternative connections are especially exposed to such pressure – a vulnerability of particular relevance to many of Australia's Pacific and Indian ocean partners, and a further reason for promoting the use of trusted networks regionally.

Taken together, these developments represent a structural – not temporary – shift in Indo-Pacific cable geography. Australia is well-positioned to benefit, but this is not automatic. The same policy settings that enhance security, including streamlined permitting, expanded protection zones, clear agency responsibilities, and a welcoming regulatory environment, are also the settings that attract investment. Getting this right is both a security imperative and an economic opportunity.

How do submarine cables work?

An understanding of how submarine cable systems work is essential to considering how vulnerabilities and threats can be best addressed. This section provides an overview of the different elements of submarine cable systems and illustrates how submarine cables are built and operate within different maritime jurisdictions. It contains the following subsections:

3.1 Submarine communications cable architecture

3.2 Submarine cables and maritime jurisdictions

3.3 Submarine cables as networks

3.1 Submarine communications cable architecture

This subsection provides background information on the architecture and elements of submarine communications cable systems, as a way of better understanding key threats and challenges. Common elements of submarine telecommunications infrastructure can be broadly divided between submarine components, terrestrial components, and terrestrial infrastructure (see Figure 10).

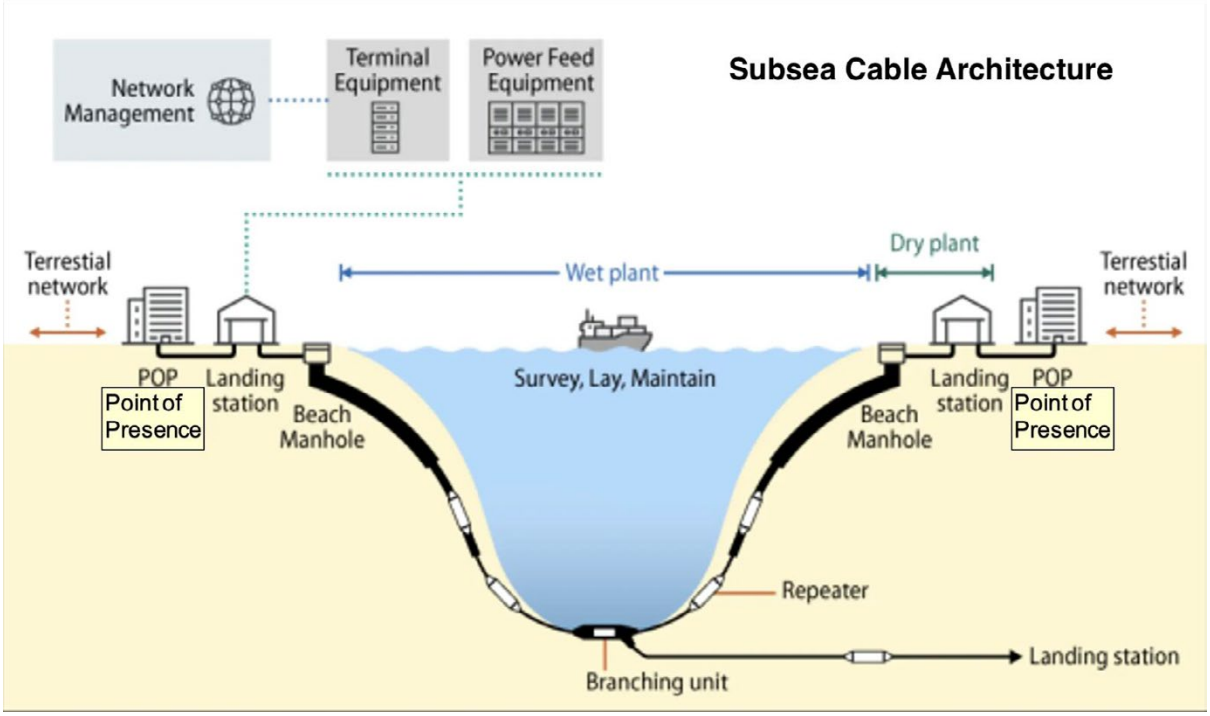


Figure 10: Elements of submarine telecommunications infrastructure. Source: Congressional Research Service, 'Protection of Undersea Telecommunication Cables: Issues for Congress', R47648, August 2023.

Submarine components

The wet components of a submarine telecommunications cable system include all elements that are placed underwater. These primarily consist of the optical fibre cable itself, repeaters, branching units, and external protective layers. The cable is carefully designed to survive the harsh conditions of the ocean, using strong materials such as steel armouring and waterproof insulation to protect the fibres that carry information. Repeaters are installed at regular intervals along the cable length to amplify the signal, and branching units enable connections to multiple landings.

Submarine cable design (see Figure 11) includes layers of armour to enhance protection in shallow and high-risk environments. In deeper waters where the risks lessen, armouring is typically not undertaken during the manufacturing process. Decisions to armour or not are made during the design process in conjunction with marine survey data analysis.

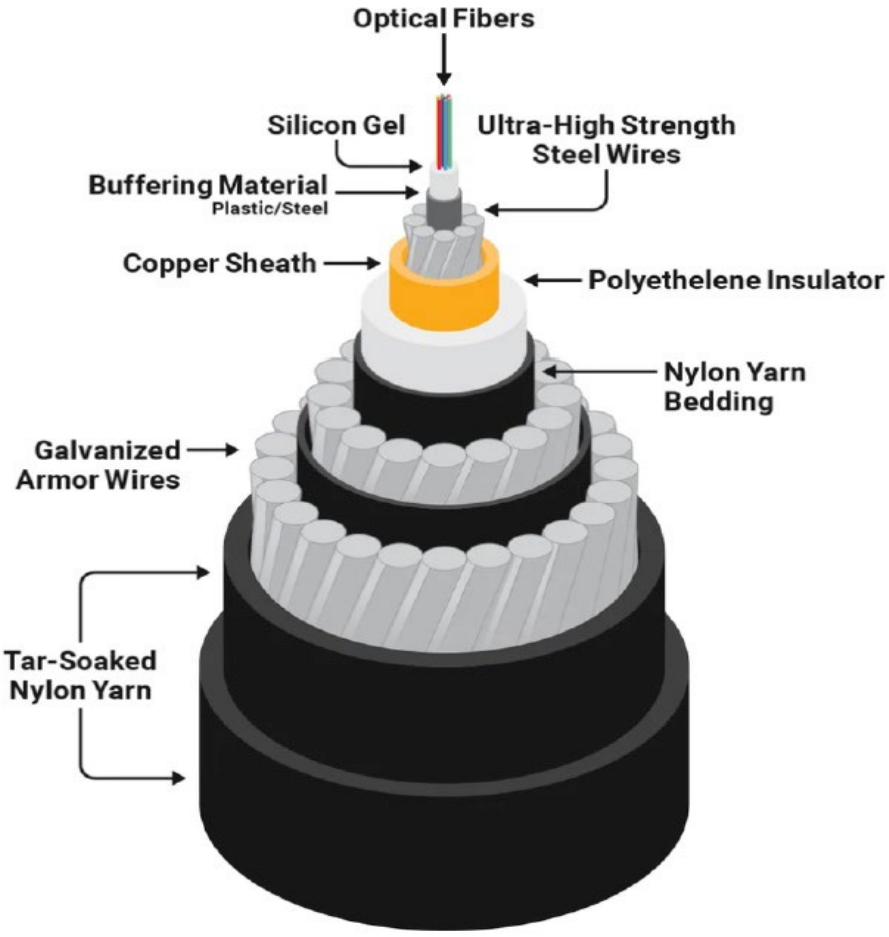


Figure 11: Submarine cable cross-section. Source: TeleGeography.

Terrestrial components

The dry components are the systems found at the Cable Landing Stations (CLS) where the submarine cable connects to local networks. These include equipment that transmits and processes data, powers repeaters in the underwater section, and tools for monitoring and controlling the cable system. Together, the wet and dry components work as a unified system to allow reliable, high-speed communications to take place.

The submarine cable emerges from the sea and terminates in a beach manhole (BMH). Underground ducts or conduits are used to protect the fibre optic cables and power cable elements between the BMH and the CLS. This infrastructure is referred to as 'fronthaul'. Underground ducts are designed to shield the terrestrial infrastructure from damage, environmental hazards, and unauthorised access. Fronthaul infrastructure is a crucial link in ensuring the continuity and integrity of the data transmission from the shoreline to the CLS.

The CLS serves as a crucial gateway between the global submarine cable network and terrestrial telecommunications infrastructure. At these facilities, the incoming optical signals from the underwater cable are received, processed, and relayed to national or regional fibre networks, enabling data to be distributed

to terrestrial service provider networks. The CLS houses sophisticated switching equipment, security systems, and backup power supplies to ensure uninterrupted service. Additionally, the CLS acts as a monitoring point for both the wet and dry components, allowing for real-time oversight, maintenance coordination, and rapid fault response. These dynamics make it an essential hub for the secure and efficient operation of network data traffic.

Network management

Each submarine cable system is managed by a Network Operations Centre (NOC), which monitors, manages, and maintains the system, including detecting faults, tracking performance (including capacity and latency), monitoring security and incident response, and coordinating emergency repairs.

Traditionally these were run by cable operators (or a lead operator of a consortium) and were located in or near a CLS, but increasingly these are located remotely (including being co-located with data centres), using remote network management systems. Remote access facilities or secondary NOCs may be configured for other consortium investors to monitor their own fibres, but a primary NOC is required for overall cable operation, maintenance and repair coordination.

The physical location of the primary NOC is increasingly an important issue for government security agencies, which may need to communicate directly with network operator personnel or require operators to act in respect of the cable.

3.2 Submarine cables and maritime jurisdictions

The transnational nature of international cables means that maritime jurisdictions – the manner in which the oceans are divided among states – have fundamental importance to the location and governance of submarine cables. The United Nations Convention on the Law of the Sea (UNCLOS) provides the basic framework for the different types of jurisdictions that littoral states can exercise over maritime spaces, including territorial waters, contiguous zones, exclusive economic zones, and the continental shelf (see Figure 12). This determines which countries can claim regulatory control over cables transiting respective waters or terminating on their territory.

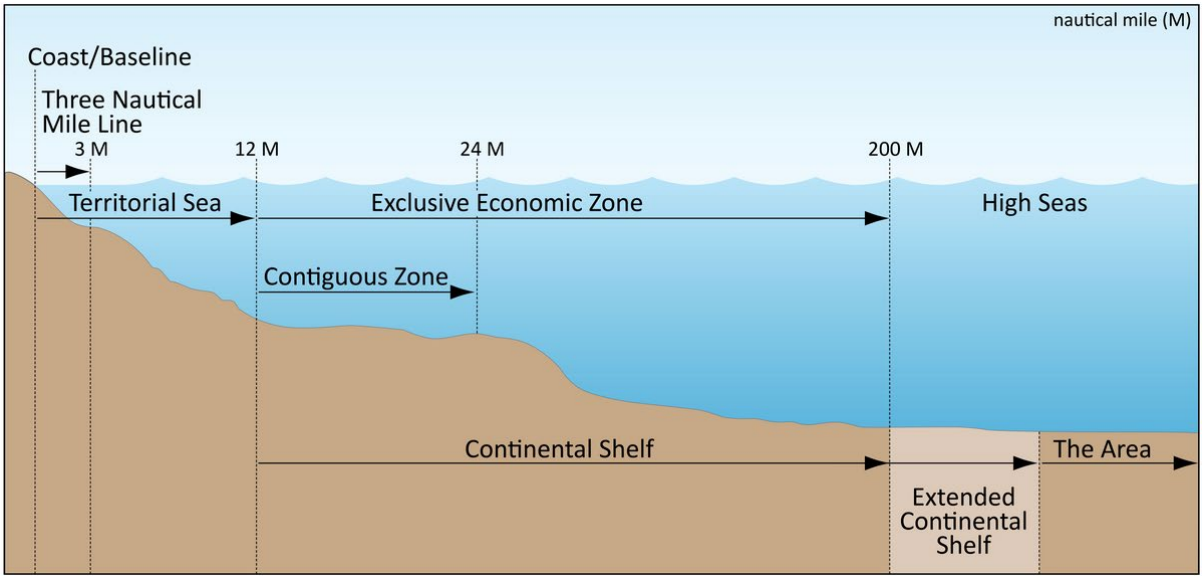


Figure 12: Maritime jurisdictions under UNCLOS. Source: US Department of State (as modified by NOAA).

UNCLOS gives all states the freedom to lay cables in the high seas, Exclusive Economic Zone (EEZs) of coastal states and in territorial seas (subject to rules of innocent passage), and requires states to adopt laws to protect cables.[27] Other international law governing cable protection, with particular reference to establishing offenses for cable damage, includes the *1884 Convention on the Protection of Submarine Telegraph Cables*, which Australia has acceded to. Both UNCLOS and the 1884 Convention are widely seen as inadequate in protecting cables from disruption from human activities, particularly in the lack of effective enforcement mechanisms. However, the reform of these treaties is likely to be difficult in light of prevailing geopolitical tensions among the major powers.

The regime of maritime jurisdictions established under UNCLOS is further complicated in Australia by overlapping state and federal jurisdictions. Under Australian law, the Australian states and the Northern Territory have primary legislative responsibility for 'coastal waters' up to three nautical miles from the coast. However, in practice federal, state, and territory laws can apply throughout the whole of the territorial sea.[28]

A sovereign state's claim to regulate cables in a certain maritime space and then its willingness to grant necessary permits on a timely basis (e.g. to undertake repair or maintenance) will impact other states that rely on a cable for international connectivity. It is important to note that UNCLOS does not explicitly authorise states to impose consent or approvals for activities beyond its territorial waters, meaning that under UNCLOS treaty obligations, consent or approvals for cable installation or repair activities are not legislated in Australia's EEZ or on the continental shelf. From an international perspective, licences or permits are required to occupy the seabed within a nation's territorial waters. Contrary to the UNCLOS treaty obligations, many nations also impose similar licences to install and repair cables within the EEZ.

Attempts by states to restrictively regulate the laying or repair of cables within their territorial waters or other waters claimed by them may cause cable operators to find other pathways. Indonesia's cumbersome regulatory regime and cabotage rules for cable maintenance vessels is causing cable operators to avoid Indonesian waters (including connections with Indonesia).[29] Similarly, China's illegal claims over the South China Sea are causing many operators to avoid laying cables in waters within the 'Nine-dash Line'.[30] Australia can benefit from legal/regulatory overreach by promoting the use of Australian territory at Christmas Island as a way of avoiding these problems.[31]

3.3 Submarine cables as networks

Submarine cable networks should not be analysed in isolation – as single systems – but are best understood as elements of a wider global digital mesh. These 600-odd networks interlink at exchange points, and packets may traverse multiple submarine and terrestrial cable systems to reach respective destinations. When submarine cable networks are offline, whether due to a fault or scheduled maintenance, data is re-routed and most customers rarely experience delays. As more submarine cable networks are installed, including via diverse routes and to new landing points, the global network becomes more resilient, and the subsea 'mesh' is strengthened. Even though the exact path a particular packet takes to its destination depends on a complex mix of commercial arrangements (and therefore does not flow like water), packets can transit multiple submarine cable networks. Therefore, a submarine cable network should be understood as one component of a larger networked system that enables packets to flow between the parts.

While the mesh structure provides inherent redundancy, this global network architecture also has concentrated points of vulnerability.

Certain geographic locations function as critical connectivity nodes or hubs where multiple cables converge, creating chokepoints through which vast amounts of international data must flow. Singapore exemplifies this concentration, serving as the primary Asian hub connecting cables from Europe, the Middle East, Asia, and Oceania. Similarly, narrow maritime passages such as the Malacca Strait and the Red Sea constrain cable routes, forcing multiple systems through limited geographic corridors. These chokepoints represent systemic vulnerabilities where a single disruptive incident can affect multiple cable systems simultaneously, degrading the resilience that the mesh structure otherwise provides.

The concentration of cable landing stations in specific locations also compounds network vulnerability. Major hubs such as Mumbai, Singapore, Sydney, Marseille, and Guam host numerous cable landing stations in relatively compact geographic areas. This concentration reflects a commercial logic – proximity to financial centres and data centres reduces costs and latency. However, it also means that localised disruptions can simultaneously affect multiple international cable systems. The cable landing station infrastructure itself – including terrestrial connections, power supplies, and network management systems – becomes a potential single point of failure despite the redundancy built into the submarine cable network. Understanding submarine cables as a network therefore requires analysing not just individual cable systems, but the geographic concentration of both maritime routes and terrestrial landing points. This understanding of how submarine cable systems work – and where vulnerabilities lie – provides the technical foundation for the governance, threat, and response analysis that follows.

Australia's approach to governance and protection

The governance of Australia's submarine cable infrastructure involves a complex interplay of private sector ownership, regulatory oversight, and strategic policy coordination. Unlike many critical infrastructure sectors where government ownership or direct control is common, submarine cables are primarily owned and operated by private telecommunications companies and, increasingly, technology hyperscalers.

Despite the critical importance of the submarine cable network to Australia's national security and economic and social wellbeing, Australia has not yet adopted a comprehensive and effective strategic and regulatory approach to the protection of its cable network. This has several consequences. The apparent lack of strategic prioritisation means that relevant security authorities have little imperative to devote significant resources to cable protection. Indeed, there is considerable uncertainty in many cases as to which agencies have formal responsibility. Regulation of cable security also remains somewhat ad hoc in certain cases, with limited legal redress for the intentional or negligent disruption of cables.

This section contains the following subsections:

4.1 Australian strategic guidance on cable security

4.2 Australian laws relating to the protection of submarine cables

4.3 Roles and responsibilities of Australian government agencies

4.1 Australian strategic guidance on cable security

Australia's key strategic guidance documents have little to say about the protection of the country's cable network. As a consequence, Australia relies on a patchwork of somewhat ad hoc regulation, with considerable uncertainties about the roles and responsibilities of relevant government agencies or the respective responsibilities of government agencies and private cable operators. Australia's 2026 *National Defence Strategy* and *Integrated Investment Program* mentions critical infrastructure protection and prioritises "undersea warfare", but does not articulate a response.[32] Likewise, Australia's 2022 *Civil Maritime Security Strategy* does not expressly address submarine cable protection.[33]

Similarly, although cyber-attack constitutes one of the most significant risks to the operation of submarine cable networks, it receives little mention in the *2023–2030 Australian Cyber Security Strategy.* Although existing Australian programs relating to Pacific Islands, such as DFAT's Cable Connectivity and Resilience Centre and the AIFFP are noted as strengthening undersea cable systems in the Indo-Pacific,[34] there is no mention of the cyber security of Australia's cable network.

The *Guide to Australia's Maritime Security Arrangements (2020)* (GAMSA)[35] does make mention of Australia's cable network, although arguably it is incomplete and inadequate. The purpose of GAMSA is to provide a practical guide to Australia's civil maritime security priorities, along with a clear statement of the allocation of responsibilities (lead and supporting) among relevant government agencies. One of the eight priority civil maritime threats identified by GAMSA is "Illegal Activity in Protected Areas", one of those areas being "protected zones declared around submerged pipelines and cables". This is a reference to the three CPZs that have been declared in Sydney and Perth.

GAMSA states that, "these [cable protection] zones are in place when the cables are less than 2,000 metres below the surface of the ocean (beyond this depth there is considered to be no appreciable threat). In Australia this means they extend up to 50 nautical miles from shore". GAMSA further states that "enforcement of maritime security zones is the responsibility of state and territory government agencies (normally water police) within coastal waters. Outside coastal waters (within

the territorial sea, contiguous zone and EEZ) enforcement responsibility rests with the MBC".

MBC is a multi-agency task force within the ABF. It is led by a Rear Admiral from the ADF and supported with capabilities from the ABF and tasked capabilities from the ADF. GAMSA identifies that MBC's role in protecting cables within CPZs in quite limited terms – being where transportation to or surveillance of CPZs is required. Although, as will be discussed below, despite this limited mandate, MBC is not currently properly resourced for this role, and nor is it resourced for broader monitoring or response capabilities.

At a strategic level, GAMSA's treatment of the protection of Australia's submarine cables is inadequate in several respects and leaves considerable gaps in perceived responsibilities of relevant Australian security agencies for cable protection.

GAMSA's focus on the three declared CPZs in Sydney and Perth fails to address the security of many existing and planned international cable connections with Australia that lie outside the CPZs. GAMSA's focus on the CPZs and the accompanying assessment that there is no appreciable threat below 2,000 metres might also be surprising to some analysts. Admittedly, it is consistent with historical statistics for times of relative peace – for example, globally, between 2010 to 2023 only 2 per cent of cable faults occurred in the high seas. However, this assessment does not appear to consider potential threats posed by well-resourced state-based actors and ignores the fact that international cables need to be protected along the entire length, whether it be in areas of Australian jurisdiction, in high seas, or areas within the jurisdiction of other countries.

GAMSA should be amended to address responsibilities for threats to cables outside of CPZs. It might be noted that, by its terms, GAMSA deals only with *civil* and not *military* maritime security threats, but it does point to a significant gap in Australian strategy and regulation.

4.2 Australian laws relating to the protection of submarine cables

Australia's approach to the regulation of submarine cables encompasses regulation of telecommunications, critical infrastructure protection, maritime spatial planning and environmental protection. The regulatory framework has evolved to address both traditional concerns around telecommunications service provision and newer challenges related to cybersecurity, foreign ownership, and infrastructure resilience.

The security of Australia's submarine cables and the data that runs across them is governed by multiple laws that are intended to protect them from damage and secure them from digital interference. Laws in this area are complex, in part reflecting the intersecting and overlapping jurisdictions of international law, federal law, and state and territory law. In our view, these laws require updating to consider the evolving nature of threats in this area and to cover some significant gaps.

The primary pieces of Commonwealth legislation including specific provisions for the protection of submarine cables are the *Security of Critical Infrastructure Act*, the *Telecommunications Act* and the *Submarine Cables and Pipelines Protection Act*. These are supplemented by general criminal laws as well as state and territory legislation.

The power of the Australian Parliament to make laws in respect of cables beyond Australian territory (including territorial waters) is constrained by international law, including UNCLOS, which provides only limited extra-territorial authority in relation to submarine cables. Within Australia's EEZ/continental shelf, for example, Australia's authority under UNCLOS is limited to making laws with respect to activities where that activity is connected to the exploration of the EEZ/continental shelf of Australia or exploiting the resources of the EEZ/continental shelf. Nevertheless, Australian courts have recognised that the Australian and state parliaments have the constitutional power to make laws of extra-territorial application.

Security of Critical Infrastructure Act

The *Security of Critical Infrastructure Act 2018* (SOCI), applies to submarine cables as part of all critical infrastructure and systems of national significance. It applies to cables installed in Australian territory and waters under Australian jurisdiction, even if they physically extend internationally, as critical telecommunications assets.

SOCI is not directly applicable to actors that may seek to disrupt Australia's submarine cables network. Rather, it imposes legal obligations for security on the relevant "responsible entity" (usually a carrier, which owns the network, or carriage service provider) to protect the "security" of the cable system as well as protecting it from other hazards. They must have a written risk management plan that they maintain and comply with, as well as a cyber incident response plan. They must notify the regulator of cyber incidents and significant network changes that would affect the asset's protection.

As critical telecommunication assets, submarine cable systems are subject to the enhanced security regulation for critical telecommunication assets under Part 2D of the Act. This requires the entity responsible for the cable to protect it so far as it is reasonably practicable from any hazard where there is a material risk of a relevant impact. This includes ensuring the "availability and integrity of the asset" as well as the "confidentiality of communications". The addition of "data storage" in the latest SOCI reforms closes a gap by ensuring that equipment such as network management servers are also covered.

SOCI requires that cable asset owners must have a Telecommunications Security and Risk Management Program to manage risks. Responsible entities are also subject to various reporting requirements. Operational changes to the network that are likely to have a material adverse effect on the entity's ability to protect its asset must be notified to the Secretary of the Department of Home Affairs. There is also a mandatory cyber incident reporting obligation under Part 2B of the Act, where a responsible entity must report cyber incidents to the ASD if they impact the asset's availability, integrity, or reliability (including data breaches that cause an operational impact).

SOCI also creates a special category of Systems of National Significance (SONS) which are (non-publicly) declared by the minister, based on criteria including that "the consequences that would arise for Australia's social or economic stability, defence, or national security if a hazard were to occur that had a significant relevant impact on the asset". Although these declarations are not publicly available, it is likely that some if not all submarine cables landing in Australia have been declared SONS. If so, these cable systems would also be subject to the Enhanced Cyber Security Obligations under Part 2C of the Act, which would create additional obligations on responsible entities such as undertaking cyber security exercises, submitting a cyber incident response plan, undertaking a vulnerability assessment, and, if required by the Department of Home Affairs, to provide system information to the ASD.

One potential gap of the current SOCI protection regime is that there is no requirement for a submarine cable system to be built secure-by-design or have adequate monitoring systems against interference. The adequacy of ACMA's regulatory authority in respect of the protection of cables may also require review.

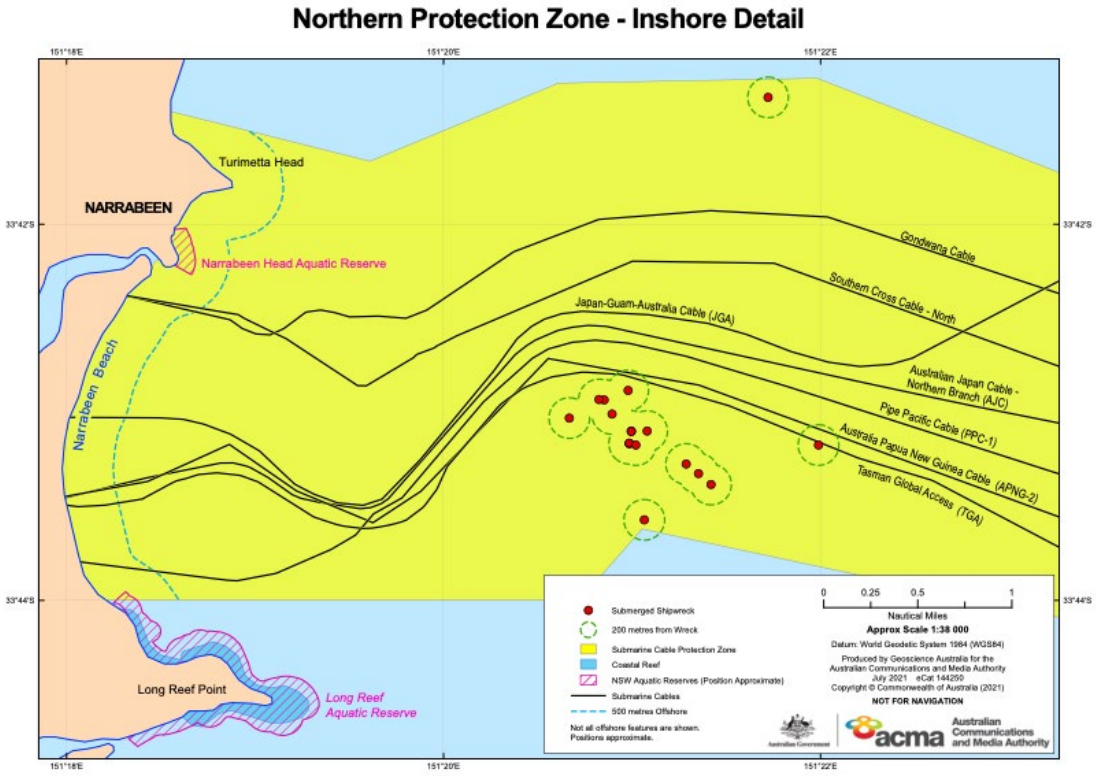
Telecommunications Act

The *Telecommunications Act 1997* includes provisions directed towards actors that may seek to disrupt certain submarine cables. Schedule 3A of the Act provides for a dedicated regime for the physical protection of selected submarine cables landing in Australia. The Act gives ACMA powers to declare specific CPZs around international cables of national significance. The Governor-General can also declare domestic cables to be of national significance.

Within these zones (but *not* outside of the zones), the Act prohibits or restricts activities that pose a high risk of physical damage to the infrastructure, such as dropping anchors, specific types of fishing such as trawling, and mining operations.

Carriers must obtain a permit from ACMA before installing new international cable in Australian waters, and the Act imposes criminal penalties on anyone who installs a cable without a permit or who damages a cable located within a protection zone. As part of the installation permit application process, ACMA consults with the Attorney-General's Department, and on security matters, the Department of Home Affairs.

Three of these CPZs have been defined so far, two in Sydney and one in Perth. Figure 13 shows two zones that have been declared off Sydney. The southern Sydney zone was recently extended southwards to include new cables landing at Maroubra Beach. Figure 14 shows the zone that has been declared near Perth.



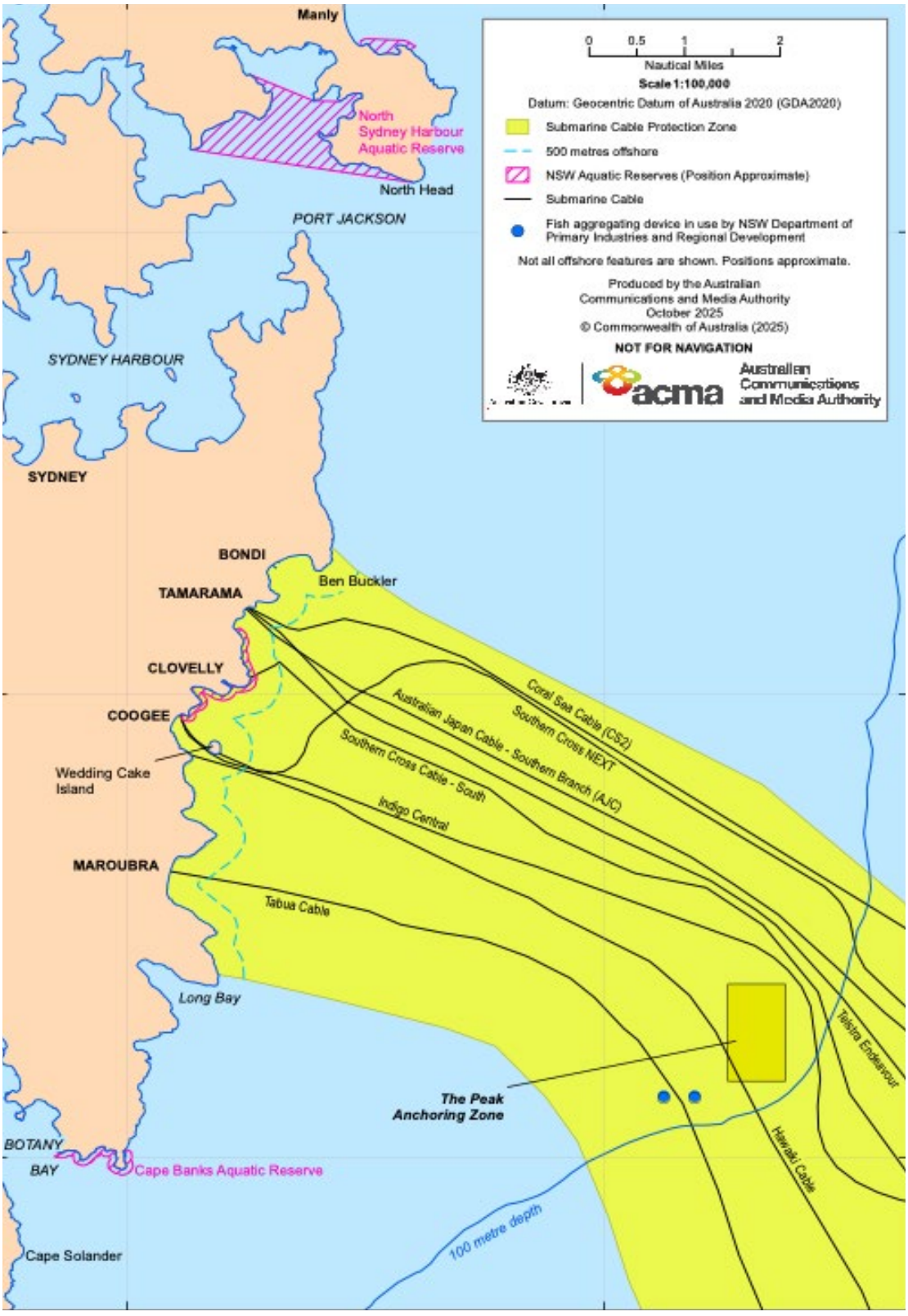


Figure 13: Sydney CPZs. Source: https://www.acma.gov.au/zones-protect-sydney-submarine-cables.

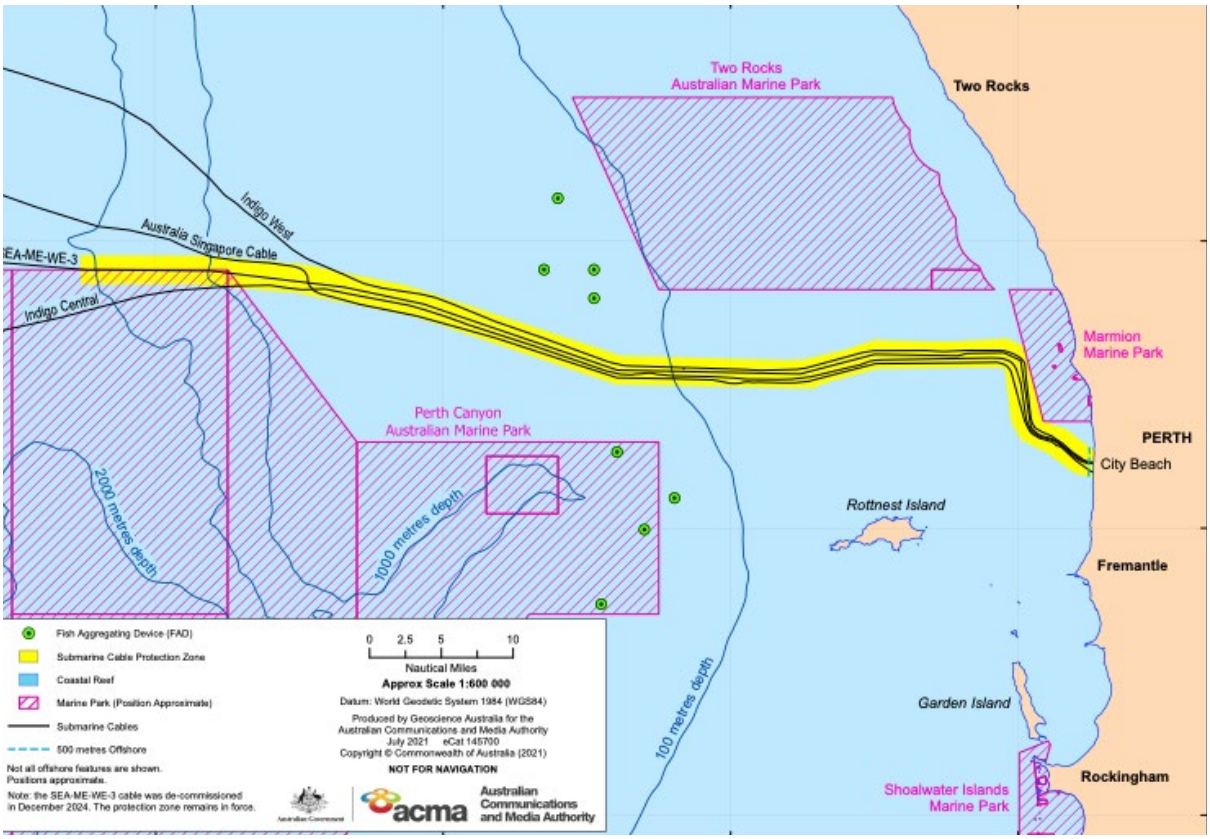


Figure 14: Perth CPZ. Source: https://www.acma.gov.au/zone-protect-perth-submarine-cables.

The penalty for damaging a cable inside a cable protection zone is imprisonment for 10 years or fines of around A$200,000. Penalties for negligent damage to cables are three years' imprisonment or fines of around A$60,000. The legislation provides for defences where the damage occurred as a result of trying to save life or ship or prevent pollution.

The CPZs nominally extend from the shoreline to waters of around 2,000m in depth (i.e. for the Northern Sydney CPZ out to about 40 nautical miles, for the Southern Sydney CPZ out to about 30 nautical miles and for Perth out to about 51 nautical miles). Despite the declaration of the CPZs under the Act, there may be significant limitations on Australia's legal authority in the CPZs beyond territorial waters. Beyond territorial waters, Australia has the power to legislate with respect to its own citizens or Australian-flagged vessels. But in relation to foreign persons/vessels may be more limited. Under UNCLOS, Australia's authority beyond territorial waters but within the EEZ is limited to activities that are connected to the exploration of the EEZ or exploiting the resources. Otherwise, Australia would be seeking to apply the *Telecommunications Act* to foreign persons/vessels on an extra-territorial basis.

Declared CPZs cover a significant proportion of Australia's submarine cables. However, the *Telecommunications Act* does not provide any legal protections for cables outside the CPZs, such as those that land in Queensland, Northern Territory, Western Australia, Christmas Island and Cocos (Keeling) Islands. As will be discussed below, this leaves a significant gap in Australia's legal regime for the protection of submarine cables.

Submarine Cables and Pipelines Protection Act

The *Submarine Cables and Pipelines Protection Act 1963* is a federal law that implements Australia's obligations under the *1884 Paris Convention for the Protection of Submarine Telegraph Cables*. The Act applies to all submarine cables beneath the high seas or in Australia's EEZ, but not to cables in Australian territorial waters, coastal waters or CPZs. It is very limited in scope and effect by virtue of the terms of the 1884 Convention, which the Act relies upon for authority.

The Act makes it an offence for an Australian citizen or an Australian registered ship to break or injure a submarine cable within Australia's EEZ or on the high seas (but not cables already covered by the *Telecommunications Act*), except where persons are acting with the sole objective of saving their lives or their ship. Limited criminal penalties apply: 12 months' imprisonment or a fine of up to A$6,600 for deliberate acts and three months' imprisonment and up to A$3,300 for negligent acts. Owners of ships may also be liable to pay for repairs of damaged cables, unless all reasonable precautions were taken. Owners of ships that sacrifice anchors or gear to avoid damaging a cable/pipeline may also be entitled to compensation.

Other federal, state, and Northern Territory laws

It may be possible to rely on federal criminal laws to prosecute persons who disrupt cables, such as provisions in the federal *Criminal Code Act 1995* prohibiting intentional interference with telecommunications facilities. Because of jurisdictional limitations, this may generally only apply within territorial waters or otherwise to an Australian person/flagged vessel.[36]

Submarine cables may also be protected by state or Northern Territory laws that apply to coastal waters (i.e. up to three nautical miles from the coast).[37] However, in practice, state and Northern Territory laws relating to submarine cables are focused on preventing unintentional damage through anchoring in enclosed waters. For example, under the Queensland *Transport Operations (Marine Safety) Act 1994* and associated rules, anchoring is strictly prohibited within 200 metres of marked submarine cables. In addition, general criminal state or Northern Territory laws prohibiting the intentional damage to property might also apply. These are likely to be of limited utility in preventing the intentional disruption of submarine cables offshore.

There are no similar applicable laws for the external territories of Christmas Island and Cocos (Keeling) Islands.

Maritime Powers Act

The *Maritime Powers Act* is intended to provide a comprehensive legal framework for Australian maritime officers such as personnel from the Navy, ABF, and Australian Federal Police (AFP), to enforce laws in the maritime domain, including laws relating to customs, migration, foreign fishing, quarantine, and drug trafficking. In broad terms, the Act empowers maritime officers to board, search, detain, and seize vessels, aircraft, or installations in the maritime domain.

Maritime law enforcement officers rely upon the *Maritime Powers Act* to define their law enforcement powers, including in the protection of submarine cables. This includes enforcement of federal laws such as the *Telecommunications Act* with respect to cables within cable protection zones and, for cables outside protection zones, the *Submarine Cables and Pipelines Protection Act* and, following authorisation, also relevant state laws. State and territory police can also be authorised to act under the *Maritime Powers Act*.

The *Maritime Powers Act* includes detailed provisions authorising maritime law enforcement officers to take various actions to ensure compliance with relevant laws, including to investigate or prevent any contravention of an Australian law that the officer suspects, on reasonable grounds, that a vessel or person is involved in.

Except as provided in the Act, a federal maritime law enforcement officer such as a naval officer may not otherwise have authority to act against a person interfering with a submarine cable whether within or outside waters under Australian jurisdiction.

Limitations or gaps in Australian laws for the protection of cables

There are some significant limitations and gaps in existing Australian laws that protect submarine cables, including due to limitations in the application of Australian laws beyond territorial waters.

Although three CPZs have been declared under the *Telecommunications Act* that nominally extend 30-51 nautical miles from the coast, Australia's legal authority beyond territorial waters may be limited. In particular, its application to foreign persons/vessels outside territorial waters may be on an extra-territorial basis.

Further, the *Telecommunications Act* only applies to cables within declared CPZs and does not provide protections to other cables. This means that cables landing in Queensland (Sunshine Coast), Northern Territory (Darwin), Western Australia (Port Headland), Christmas Island, or Cocos (Keeling) Islands, for example, do not gain the benefit of protection under the Act.

State and Northern Territory laws specifically for the protection of submarine cables may apply to cables in coastal waters and, potentially, also territorial waters. However, these tend to be very limited and may be difficult to enforce. There are no analogous "territorial" laws in Christmas and Cocos (Keeling) Islands.

The *Submarine Cables and Pipelines Protection Act 1963* only applies outside the protection zones and the territorial sea, and even then, only to Australian-flagged vessels. Outside of the protection zones the *Maritime Powers Act,* combining with *Crimes (Ships and Fixed Platforms) Act 1992* s23 or the *Criminal Code* s474.6, would provide for Commonwealth enforcement action, including within the territorial sea, even if prosecution could be difficult. The *Maritime Powers Act* refers to breaches of Australian law. It explicitly includes state and territory law (section 8). One could therefore have the ADF, ABF, or AFP enforcing any state law. Here it would be a case of seeing if there were relevant offences applicable by virtue of state law out to 12 nautical miles, or beyond by virtue of the *Crimes at Sea Act 2000*. So, it is possible to have a contravention authorisation under s17 of the *Maritime Powers Act* for an offence against a state or territory law. It would then be a question of whether the Attorney-General would authorise a prosecution under s7 of the *Maritime Powers Act.*

Further, where a foreign vessel that is involved in disrupting a submarine cable has sovereign immunity (e.g. it is a warship or other non-commercial vessel owned by a foreign state), then the authority of Australian law enforcement officers may be even further limited, in which case the Australian Government may need to rely on its executive powers for the defence of the Commonwealth.

These jurisdictional limitations could present real problems for maritime law enforcement authorities. For example, in October 2025, a Finnish court dismissed sabotage charges against the crew of the *Eagle S*, a Russian-linked tanker suspected of severing five critical Baltic cables. They did so on jurisdictional grounds: the incident had occurred beyond Finland's territorial waters. Moreover, the vessel's flag state, the Cook Islands, had not initiated any proceedings. It is not clear if an Australian court would take a more robust view of the reach of Australian law.

4.3 Roles and responsibilities of Australian government agencies

The governance of submarine cables in Australia involves multiple government agencies with overlapping responsibilities. Figure 15 summarises designated responsibilities of relevant federal and state agencies.

Agency	Roles and Responsibility
Department of Prime Minister and Cabinet	Responsible for building national resilience, leadership and coordination across Commonwealth government agencies.
Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts	Policy lead for communications regulatory issues. Administers the *Telecommunications Act*.
Australian Communications and Media Authority	Regulatory authority over CPZs. Permitting of new cables (in consultation with Home Affairs). Lead agency for the prohibition and restriction of activities in CPZs (GAMSA).
Department of Home Affairs (Critical Infrastructure Security Centre)	Policy lead for domestic security. Administers the *Security of Critical Infrastructure Act* (SOCI).
Maritime Border Command (Home Affairs Portfolio)	Transportation to and surveillance of CPZs (GAMSA).
Australian Border Force (Home Affairs Portfolio)	Enforcement or transportation as required (GAMSA).
Australian Defence Force (including Royal Australian Navy)	Protects critical infrastructure as part of responsibilities for Subsea and Seabed Warfare. Provides enforcement, transportation or surveillance as required (GAMSA).
Australian Signals Directorate (Australian Cyber Security Centre)	Cyber incident assistance and response.
Department of Foreign Affairs and Trade	DFAT's Cable Connectivity and Resilience Centre supports governments in the Indo-Pacific to apply best practice in the development and reform of cable policy and regulatory frameworks. Represents Australia on international issues/organisations including: International Cable Protection Committee International Telecommunication Union International Advisory Body on Submarine Cable Resilience engagement with regional partners international agreements.
Australian Federal Police	Responsible for investigating incidents involving damage to cables, particularly within designated protection zones and on land under applicable federal statutes. Provides armed law enforcement and assistance with prosecution as required (GAMSA).

Agency	Roles and Responsibility
State and territory police	Responsible for investigating incidents involving damage to cables, within coastal waters (up to three nautical miles) as well as landing points and terrestrial infrastructure under applicable state statutes. Provides armed law enforcement and assistance with prosecution as required (GAMSA).
Australian Hydrographic Office, Department of Defence	Undertakes hydrographic surveys and maintains nautical charts. Issues Notices to Mariners on location of submarine cables.
Federal Attorney-General's Department	Provides government legal direction as required. ACMA must consult department before granting installation permits. Attorney-General's consent required to bring certain legal proceedings against foreign nationals or regarding acts committed outside Australia.
State and territory governments	Responsibilities for marine spatial planning as well as coastal zone permits for cables and cable landing stations outside a CPZ.

Figure 15: Roles and responsibilities of Australian agencies for the regulation of submarine cables.

While there is a degree of informal coordination among relevant federal and state agencies, including an Interdepartmental Committee on submarine cables, the lack of strategic guidance from the Australian Government undermines the clear allocation of key responsibilities among agencies.

JAMAG is a high-level interagency coordination committee, chaired by Commander MBC, which brings together government agencies to coordinate whole-of-government maritime security efforts, assess risks, and detect and combat threats within the maritime domain. We have recommended that JAMAG be given principal responsibility for the coordination of policy and operational responses among relevant agencies in respect of submarine cables. We have also recommended that the committee should report regularly to the Secretaries Committee on National Security on threat developments and cable network security.

Taken together, the governance gaps identified in this section – in strategic guidance, legal frameworks, agency responsibilities, and coordination mechanisms – underscore the need for the comprehensive national approach to submarine cable protection that this report recommends.

Risks, vulnerabilities and threats

Submarine cables are subject to a range of physical and digital threats. Physical threats include environmental factors, unintentional disruptions from human activities, and intentional attacks. Digital threats include cyber-attacks and unauthorised data interception.

Australia has experienced relatively few significant disruptions to cable connectivity in recent times due to its geography and other factors. However, during both world wars, adversaries attempted to cut Australia's cable communications with the outside world, and a future adversary might also take advantage of any vulnerabilities.

This section examines the risks and threats faced by submarine cables around the world. It contains the following subsections:

5.1 Environmental threats

5.2 Unintentional disruptions from human activities

5.3 Intentional attacks in the maritime environment

5.4 Threats to submarine cables in the terrestrial environment

5.5 Cyber threats

5.6 Australia's experience

5.1 Environmental threats

Worldwide, around seven per cent of all cable breakages are caused by natural factors (see Figure 16). Cable disruptions can be the outcome of natural disasters such as seaquakes and other seismic activity, tsunamis, and underwater currents during storms. Further natural factors are long-term processes that may lead to abrasion of the protective layers of cables, such as corrosion, tide, and weather-related currents.

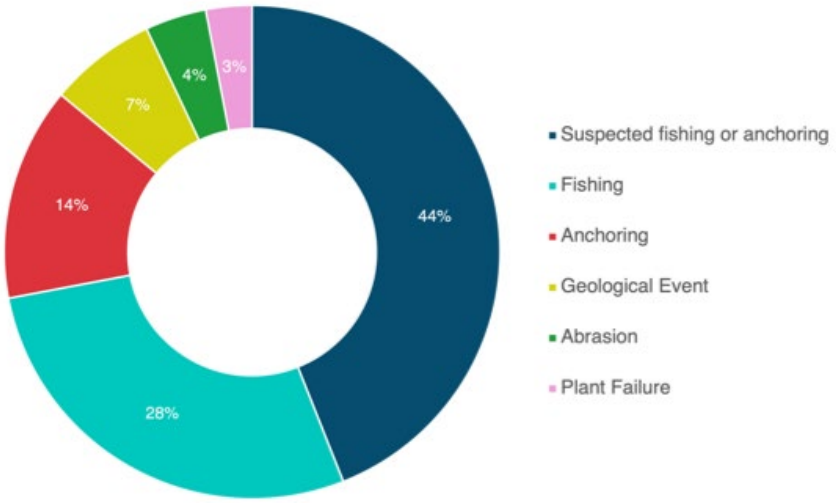


Figure 16: Causes of submarine cable faults.
Source: International Cable Protection Committee (ICPC) Global Repair Data 2025.

Although environmental threats are less likely than disruptions from human activities, they still have the potential to cause the simultaneous failure of multiple cables, with significant consequences for affected countries. For example, the 2006 earthquake near Taiwan severed multiple trans-Pacific cables and reportedly disrupted 90 per cent of internet traffic around Asia.[38] Due to the Japanese earthquake of 2011, four of 20 submarine cables to Japan ruptured. More recently, undersea currents caused by a volcanic erup-

tion near Tonga in 2022 took out both Tonga's international and domestic cables. International connectivity was restored after five weeks, but it took 18 months for the domestic cable to be restored because the scale of damage exceeded available spare cable and required cable to be manufactured.

In comparison with some other countries, Australia has a relatively low level of cable disruptions from environmental causes. This is helped by Australia's location near the centre of the Indo-Australian tectonic plate, meaning there is a relatively low level of seismic activity in Australian waters.[39]

5.2 Unintentional disruptions from human activities

'External aggression' is a term used by the submarine cable industry to describe threats arising from human activities or interventions. It describes incidents that may be deliberate or not and the term does not necessarily imply intentional sabotage. Human activities (mostly unintentional) are the cause of around three quarters of all cable faults.[40]

Demersal fishing, or bottom trawling, is considered a primary risk to cables due to otter boards contacting the seabed, especially where cables are seabed laid (see Figure 17). Buried cables may also be threatened if the weight of otter boards and resulting seabed penetration exceeds the burial depth. This risk can be addressed during the early planning stages of cable system development and construction, when cable armouring and burial parameters are determined.

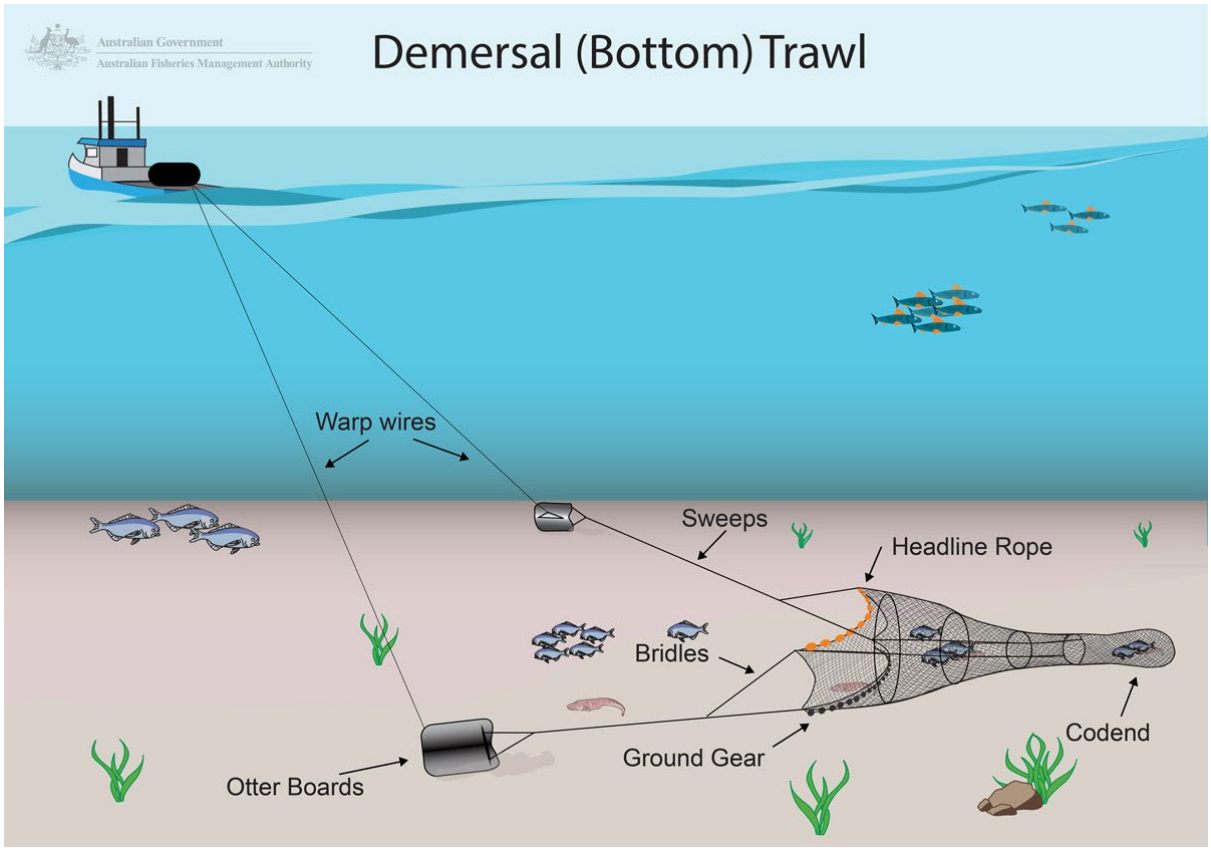


Figure 17: Demersal fishing technique. Source: Australian Fisheries Management Authority.

Because of the relatively small size of Australia's commercial fishing fleet, there is a relatively low level of external aggression risk from fishing in Australian waters – although the threat remains to Australia-connected cables from fishing activities beyond Australian waters. However, anchoring of vessels in proximity to submarine cables represents a notable threat, especially when anchors and chains possess sufficient mass to penetrate the seabed. This is particularly the case around major ports such as Sydney and Fremantle.

Current and planned cables are buried at least 1–1.5 metres under the seabed down to 1,500 metres water depth, which greatly reduces risk. These burial practices are consistent with industry protection standards, although increasingly cables are being buried up to three metres under the seabed in high-risk areas.

Marine spatial planning – the process by which governments coordinate competing uses of the seabed – is an important tool for cable protection. Offshore wind, aquaculture, shipping lanes, resource extraction, and submarine cables increasingly compete for the same coastal and shelf waters. Seabed mining activities – whether in the high seas or areas under Australian jurisdiction – may also increasingly represent a threat to submarine cables. Australia should ensure that cable operators are formally included in all relevant marine spatial planning processes, and that new offshore developments – particularly offshore wind projects, which are expanding rapidly in Australian waters – are required to coordinate with cable operators from the earliest stages of planning.

5.3 Intentional attacks in the maritime environment

Many states and non-state actors possess the power to inflict harm on maritime infrastructure. For more than a century, states have attacked submarine cables used by adversaries in times of conflict.

Historical incidents involving Australia

During both world wars, adversaries sought to cut Australia's international cable communications. In September 1914, two German naval cruisers attacked and severely damaged the telegraph station at Fanning Island (now part of Kiribati) and cut the telegraph cable. This cut Australia's only trans-Pacific communications for two weeks.[41]

Australia's first major naval battle occurred in November 1914 when the German cruiser SMS *Emden* was intercepted and sunk by HMAS *Sydney* near Direction Island in the Indian Ocean (part of what is now Australia's Cocos (Keeling) Islands territory). The *Emden* was caught and surprised by the *Sydney* in the process of destroying a vital communications link with India and Britain (Figure 18). The *Emden* had put ashore a naval landing force on Direction Island with the intention of destroying the telegraph repeater station as well as cutting telegraph cables in the island's lagoon. Despite the attack, the station and telegraph cable were only out of operation for a brief period. Among other things, the landing station staff had managed to avoid the telegraph cable being cut by laying a spare, inactive, cable in the island's lagoon to attract the attention of possible attackers.

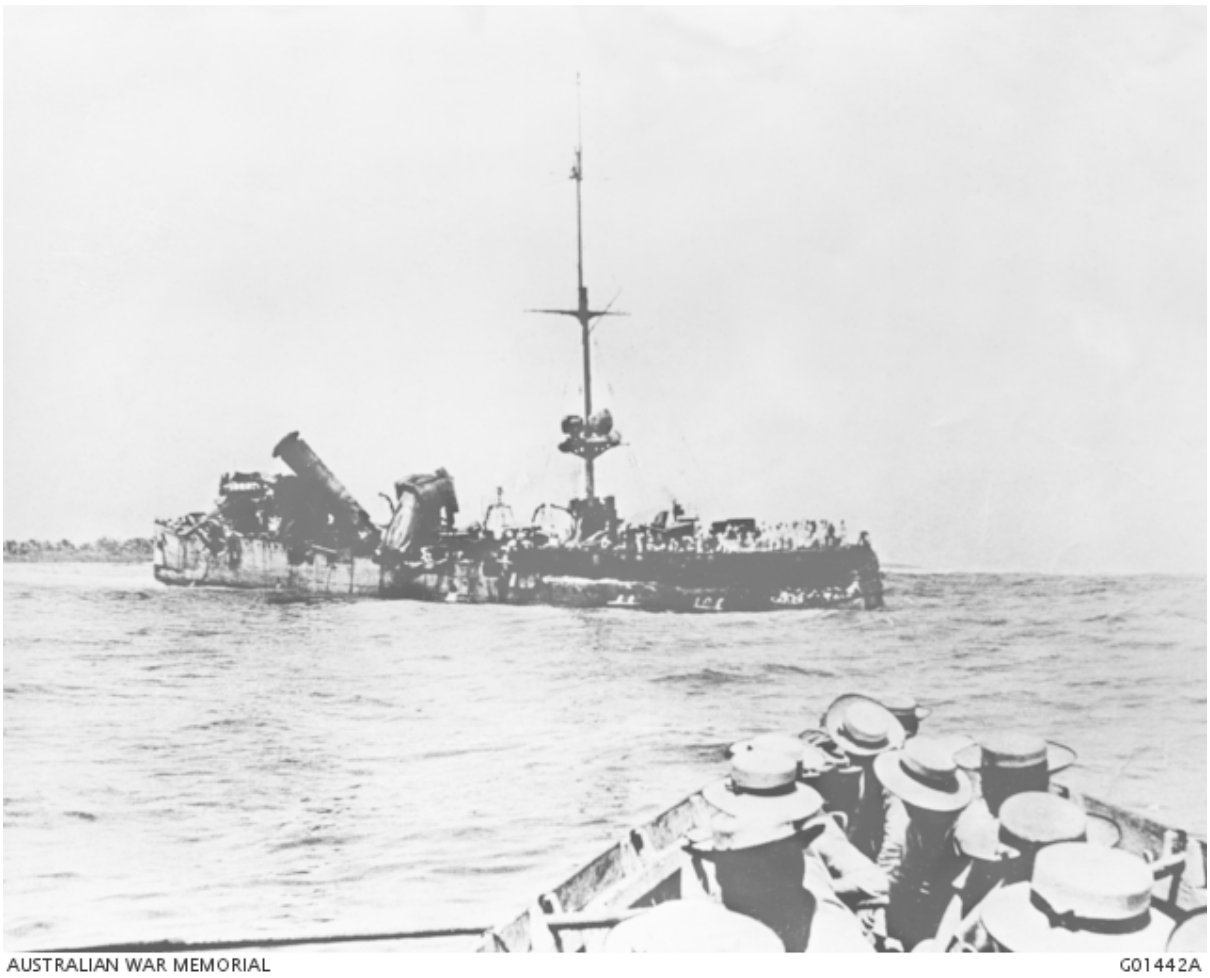


Figure 18: The wreck of the SMS Emden at North Keeling Island in 1914. Source: Australian War Memorial.

Australia was also involved in cable wars with Japan during World War II. In February 1942, when Japanese forces invaded Singapore, they immediately severed Australia's main international telegraph connections with Britain. This left Australia with only a trans-Indian Ocean cable through Cocos (with onward connections to India, South Africa and Britain) and a trans-Pacific cable to Canada. Japanese naval vessels bombarded the cable station at Direction Island in Cocos several times between February and December 1942, and the island was the target of regular air raids between 1942 and 1944. Although false messages were broadcast that the landing station had been put out of action, these attacks were not successful in severing Australia's key remaining communications link with Britain.

Australia was also involved in offensive operations against Japan when a joint British-Australian naval force cut several critical communications cables used by Japanese forces in Southeast Asia. In July 1945, as part of Operation Sabre, Australian naval personnel conducted a successful attack on submarine cables used by Japan connecting Saigon with Hong Kong and Singapore using an X-craft midget submarine. Days later, as part of Operation Foil, another British crew operating an X-craft submarine cut cables between Hong Kong and Singapore.[42]

Recent reported incidents in northern European waters

In recent years, there has been a resurgence of what appears to have been intentional attacks against submarine cables as part of hybrid or 'grey zone' operations. These incidents have occurred in northern Europe and around Taiwan. Although there have been several incidents of cable disruptions in the Red Sea in recent years that were initially attributed to Houthi insurgents, subsequent investigations showed that these were likely unintentional.[43]

As will be seen, among the key issues in

addressing these and other disruptions to cable systems are problems of intention and attribution. How should security agencies respond when attribution of foul play is probable but not certain? How can security agencies avoid mixed and contradictory messages considering these uncertainties when they are seeking to project a message of deterrence to bad actors? There are no simple answers to these questions.

Over the past five years, there have been multiple incidents involving cables and other undersea infrastructure in European waters which have, to varying degrees, been attributed to Russia. Many of these incidents have occurred off the coast of Norway or in the Baltic Sea, where many cables cross the shallow waters and Russian ports are nearby.

In April 2021, the Norwegian Ocean Observatory in the Norwegian Sea was put out of service after a 12-tonne section of underwater communications and sensing cables along with relay equipment was cut at a water depth of around 250 metres and dragged some 11 kilometres out of position. According to public reports, on inspection it was clear that a section of the cable had been cleanly cut as if with a power saw. A review of Automated Identification System (AIS) data also showed that a Russian-flagged trawler had passed back and forth over the cable at least four times at the time of the incident.[44]

In January 2022, cables connecting Norway's mainland with a satellite station on Svalbard island were severed. The cable was cut in an area where water depths are some 2,700 metres. The cable had been buried in the seabed to a depth of some three metres and on inspection there were multiple deep gashes in the seabed. Norwegian authorities took the position that there was insufficient evidence to attribute the cause of the break. However, AIS data showed that a Russian trawler, the *Melkart-5*, had crossed the cable some 130 times around the time it was damaged.[45]

In September 2022, the Nord Stream 1 and 2 submarine natural gas pipelines connecting Russia with Germany were sabotaged. Three explosions were reported, which destroyed three pipelines and released methane into the Baltic Sea. The perpetrators are yet to be identified and may not have been Russian.

In October 2023, the Baltic Connector, a natural gas pipeline connecting Finland and Estonia, and three submarine cables were damaged when the Hong Kong-flagged and Chinese-owned *Newnew Polar Bear* cargo ship dragged its anchor over a period of nine hours (the anchor was later found on the seabed next to the gas pipeline). Finnish authorities declared that the damage could not have occurred by accident as the ship's captain could not have failed to realise he was dragging an anchor for hundreds of kilometres.

In November 2024, the Chinese-flagged bulk carrier *Yi Peng 3* dragged its anchor while traversing the Baltic Sea, severing two submarine cable networks. The *Yi Peng 3* was intercepted by Danish and other European naval vessels. Investigators believed the *Yi Peng 3* severed both cables by intentionally dragging its anchor for over 160 kilometres in mild weather conditions.

In December 2024, the Cook Islands-flagged oil tanker *Eagle S* cut two submarine communications cables and one submarine electricity cable in the Baltic Sea with a dragging anchor. Finnish authorities seized the *Eagle S* and in January 2025 a court rejected a request by the United Arab Emirates-based owners to release the vessel.

In January 2025, the Sweden-Latvia cable was damaged by a dragging anchor, with two vessels identified as the possible causes. However, investigations were inconclusive and it may have been an accident.

In April 2026, the UK Government revealed that three Russian submarines had recently conducted a covert operation over cables and pipelines in waters north of the UK, including in the UK's EEZ. According to the UK Defence Secretary, Russia had sent an Akula class submarine as a diversionary tactic while two of its GUGI spy submarines carried out the surveillance of these cables, while the UK Government deployed a warship and aircraft to monitor and deter Russian activity. The British Defence Secretary, John Healey, stated: "To President Putin, I say, 'We see you. We see your activity over our cables and our pipelines, and you should know that any attempt to damage them will not be tolerated and will have serious consequences'." [46] This public statement represented a significant change to the UK Government's previous discreet approach to activities of this nature.

The great majority of these incidents occurred in relatively shallow waters, although the 2022 Svalbard incident occurred in waters some 2,700 metres deep. While many of these incidents could not be definitively attributed to Russia, there are several reasons to believe that Russia was responsible for some of them. Indeed, the problem may be wider than has been publicly reported. According to one senior German political leader, between February 2022 and December 2023, at least 25 per cent of all trans-Atlantic cables serving Europe had been out of service, commenting further that "I don't believe they were all fishing nets".[47]

Recent reported incidents in Taiwanese waters

Numerous incidents have also occurred in Taiwanese waters, many of them involving Chinese vessels. Submarine cables connecting Taiwan with its Matsu Islands, located just off China's mainland, were severed some 27 times between 2018 and 2022.[48] Chinese sand dredgers, which routinely dredge Taiwan's waters, are often responsible for the cable damage. There have been several new disruptions since then, with Taiwan alleging that at least some are not accidental.

In January 2025, the *Vasiliy Shukshin,* a Russian-owned and Belize-flagged cargo vessel, spent three weeks 'suspiciously' criss-crossing waters near the landing points of key international cables in southern Taiwan, although the cables were not apparently damaged.[49] In that same month, the Trans-Pacific Express cable connecting Taiwan with the US was damaged off the coast of Keelung by the *Shunxing 39*, a Chinese-crewed freighter. The ship had criss-crossed the cable repeatedly while dragging its anchor. Several days later, a Mongolian-registered vessel was escorted from Taiwan waters by Taiwanese authorities after it was spotted criss-crossing an area off northern Taiwan where there was a high concentration of cables.[50]

In February 2025, a cable between Taiwan and one of its outlying islands was severed by a dragging anchor of the Togo-flagged, Chinese-owned and -crewed freighter, *Hong Tai 58.* The Taiwan Coast Guard intercepted the vessel and in June 2025 the Chinese master was sentenced to three years in a Taiwanese prison for deliberately severing an undersea cable off the island. The court found he had ordered crew members to lower the ship's anchor into waters off south-western Taiwan where he would have known anchoring was prohibited because it could damage the submarine cable.

By contrast, the Chinese captain of the *Min Lian Yu 60138*, whose net and anchor damaged a cable connecting Taiwan with an outer island in October 2025, received a three-month prison sentence, commutable to a fine, for negligent damage to the cable.[51]

Overall, many of these incidents, particularly the incidents occurring in early 2025, point to possible intentional acts by the Chinese state, potentially in collusion with Russia. All these incidents appear to have occurred in relatively shallow waters. It is also interesting that, with the exception of the severing of the Trans-Pacific Express cable, all other publicly reported disruptions were to cables connecting Taiwan with its outer islands.[52]

In October 2025, the Taiwan legislature amended several laws relating to subsea infrastructure (including telecommunications, electricity, gas, and water supply) to significantly increase penalties for intentional damage, including confiscation of vessels and imprisonment for up to seven years.[53] The Taiwan Ministry of Foreign Affairs also launched its RISK Management Initiative on International Subsea Cable, which provides a road map for managing risks and threats to cables.[54]

In December 2025, the Taiwanese Government announced that Taiwan would construct two new international and three new domestic cables as part of a broader strategy to strengthen the resilience of its national communications infrastructure.[55] This would likely involve subsidies for Chunghwa Telecom, the Taiwanese national telecommunications operator. The new cables will feature an 'armour-like' protective layer designed to reduce the risk of damage from natural disasters or external interference. Taiwan will also deploy a Submarine Cable Automatic Warning System (SAWS) on selected domestic and international subsea cables, which automatically sends alerts to nearby ships and warns them not to drop anchor. As part of the same strategy, Taiwan plans to integrate low Earth

orbit (LEO) satellite capacity through Amazon's satellite constellation and launch a high-orbit geosynchronous satellite built by US manufacturer Astranis. These satellite systems intend to provide backup connectivity if terrestrial or subsea networks are disrupted.

The pattern of incidents in European and Indo-Pacific waters carries direct implications for Australia's defence planning. Historical precedent – from the German attacks on telegraph cables in 1914 to Japan's severing of communications links in 1942 – demonstrates that submarine cables are among the first targets in any conflict involving Australia. The more recent incidents in the Baltic Sea and around Taiwan suggest that state actors are now actively probing and testing cable infrastructure in peacetime as part of broader hybrid warfare strategies, with the intention of being able to rapidly degrade connectivity at the outset of a conflict. For Australia, this means that cable protection cannot be treated solely as a civil infrastructure matter. The ADF must incorporate the defence of submarine cable infrastructure into its operational planning, and Australia's broader strategic posture must account for the likelihood that its cables would be early targets in any serious conflict in the Indo-Pacific.

5.4 Threats to submarine cables in the terrestrial environment

The terrestrial elements of submarine cable systems – including the BMH, network fronthaul components, data centres and CLS – face greater vulnerability to interference because these are easier to access than the subsea components. The reconstruction of CLSs may also be a considerably lengthier and more expensive exercise than the repair of cables.

In 2021, reports surfaced that suspected Russian operatives had mapped cable landing stations across Western Europe, raising concerns about potential future sabotage efforts.[56] During the recent US-Iran war, Iran attacked data centres in Bahrain and Dubai and reportedly threatened to target cable landing stations.[57]

In Australia, BMHs for international and domestic cables are generally hidden and secured in locations that are unlikely to experience physical disruption from either human activity or natural causes, such as within carparks, or road carriage ways.

CLSs are key vulnerability points for submarine cable systems as they interconnect submarine cables with terrestrial optical fibre communication (OFC) networks and contain vital transmission, power, and network management equipment. The density of cables in one location compounds the impact of any natural or human disruption. Traditionally, cables would land at a BMH and connect to landing stations, which would then interconnect with terrestrial OFC networks to provide connectivity to data centres or telecom interconnection Points of Presence (PoP). Where geographical distances allow, newer cable systems may connect directly from the BMH to the data centre, eliminating the need for a dedicated CLS.

Geographically isolated landing stations with limited physical security may be a target for sabotage or physical entry for data exfiltration by intelligence operatives or their proxies, such as a trusted insider. Foreign landing stations in foreign jurisdictions where access control is more difficult to manage can also pose a security vulnerability.[58]

5.5 Cyber threats

Cyber represents a separate domain of potential threats to submarine cable systems. While in recent years much focus has been given to physical threats to cables, cyber arguably represents a potentially greater threat to the uninterrupted operation of cables.[59] Unlike physical attacks, which can be difficult to undertake and may carry greater risks of provoking retaliatory action, cyber-attacks can be conducted more covertly and remotely, making these tactics an effective strategy for states to disrupt the transmission of data across subsea cable infrastructure or to disable key service providers such as cable maintenance vessels. As one informed source commented, while the cyber vulnerability of submarine cables is similar to that of other critical telecommunications assets, disruption of submarine cables may carry greater strategic or symbolic value for potential adversaries.

Submarine cable systems share characteristics with other critical infrastructure that allows digital control of operational technology, making them vulnerable (in insecure network architectures) to attacks that cause physical harm through digital means. The Stuxnet worm, which used software to destroy industrial centrifuges, showed that this kind of attack is not theoretical. A cyber intrusion that allows an attacker the control to disable access to a cable system, or manually override safe operating procedures or built-in safeguards, causing the physical destruction of large parts of the system, would cause a prolonged outage, far longer than the weeks it typically takes a repair ship to locate and fix a conventional cable fault. As noted previously, when a long section of Tonga's domestic cable was destroyed by a volcanic eruption, it took almost 18 months to restore connectivity. The delay was not due to vessel logistics, but rather the damaged length exceeded available spare cable, and replacement cable and repeaters had to be manufactured and delivered before repairs could begin.

There are three main cyber risks to cable systems – those that compromise confidentiality, integrity, or availability of the data. That is, an adversary can seek to intercept and collect the data; manipulate, divert, or undermine trust in the data; or damage the system and disrupt the service and flow of data. The only publicly reported example of a cyber-attack on a submarine cable system to date occurred in April 2022, when the US Government revealed it had thwarted an attack on a telecommunications company managing a trans-Pacific submarine cable linking with Hawaii.[60] This attack was enabled by a credentials-related breach. It is likely that there are other cases of cyber-attacks on submarine cable networks that have not been publicly reported.

Submarine cables rely on onshore equipment to transmit and receive optical signals and power the transmission and repeaters. This equipment is centrally monitored and controlled by a software platform known generally as a Network Management System (NMS). Historically, these networks were isolated from the internet and accessed locally via secure enterprise networks. Today, for greater efficiency and due to work-lifestyle changes, engineers manage these global networks remotely by accessing enterprise networks over the internet. While the NMS is usually segregated from broader corporate systems, this shift to remote access significantly expands the attack surface for unauthorised access.

For commercial subsea networks, it is also common industry practice for third-party software vendors to have remote access to the network to carry out equipment updates. This has caused issues in the past as any change to systems or human interaction with the system comes with risk. It is not unheard of for cable faults to be triggered by software updates, such as a planned system upgrade on the Southern Cross Network in 2012 that caused a 70-minute outage.[61]

This is not just a problem for the submarine cable industry. For instance, in 2024 a bug in the software update for the widely used CrowdStrike Falcon software platform triggered IT disruptions worldwide. By causing widespread failures to the host Windows operating system, the update paralysed computer systems, including those used in critical infrastructure and essential services such as emergency response[62] and transportation networks.[63]

While human error can cause significant outages, more concerning is the possibility that threat actors can exploit these legitimate access methods to interfere with, steal data from, or cripple the systems of a network operator. In a worst-case scenario, threat actors could breach the networks of multiple cable operators and pre-position themselves for a coordinated attack on multiple carriers simultaneously.

The risk of cable disruption through hacking may be magnified by poor security practices from cable operators or equipment. Many remote network management systems run on widely used operating systems such as Linux or Microsoft Windows – a double-edged consideration since although these platforms benefit from regular update patches and large security communities, their ubiquity also makes them familiar territory for malicious actors. Highly specialised or obscure operating systems offer less attacker familiarity, but also a smaller community to scrutinise its security. Additionally, the mechanisms through which vendors update and can control systems once deployed on the customer end may introduce other kinds of risks into this part of the cable supply chain.

Cable maintenance vessels may also be the target of cyber-attacks. Indeed, the headquarters of one of the leading international cable maintenance groups has previously been the subject of a distributed denial-of-service attack. While ship owners are required by the International Maritime Organization to incorporate maritime cyber risk management into their safety management systems,[64] it is up to ship owners to properly implement this mandate, and relevant expertise is scarce.

Data interception

Submarine cables systems are prime targets for espionage, as they can carry vast amounts of government, military, financial, and other sensitive data. During the Cold War, as part of Operation Ivy Bells, US intelligence services famously tapped Soviet Navy transmissions by collecting data off the copper submarine cables, with recordings of communications periodically retrieved by US Navy divers.

Tapping modern fibre-optic cables underwater would present much greater challenges compared with Cold War days. Unlike the coaxial cables of old that transmit electrons and generate magnetic fields, fibre-optic cables transmit photons of light that cannot be as easily captured without penetrating the cable and disturbing the transmission (or more precisely, the optical signal to noise ratio). However, it is claimed that major state actors possess the necessary technology to conduct data interception operations. For example, the Russian submarine *Losharik* and intelligence vessel *Yantar* are said to be capable of deploying remote-operated vehicles to tap or manipulate fibre-optic cables.[65] The US nuclear submarine *Jimmy Carter* is also reported to have the capability to tap submarine cables.[66] If such tampering occurs, network monitoring systems may or may not detect the anomalies, depending on the network's link loss budget.[67]

With new submarine cables hitting transfer rates of 400 terabits per second, some industry experts suggest that collection and storage of data would be a hurdle to cable tapping as modern cables transfer a huge amount of data very quickly. However, it is not necessary for bad actors to capture all the data on the cable. Cables are stripped out into individual optical fibres as part of a cable repair within cable repeaters that amplify the signal on long-haul routes and within branching units. At these points they could be susceptible to interception.

In 2018, Japan's Ministry of Internal Affairs and Communications showed pictures of a wiretap device attached to a submarine cable amplifier, reportedly Chinese in origin, to a major Japanese communication company, which was then asked to improve inspection on its cables.[68] According to one report, the bugging device was "black, rectangular and about the size a person could carry". [69] It is not clear from public reports how exactly this device functions, nor how it found its way into the amplifier.

In theory, data flowing through fibre-optic cables can be captured by creating a physical access point that diverts a small amount of the light signal into a separate receiver, generating another copy of the light signal without disrupting the receipt of the original signal.[70] Commercial hardware is available for terrestrial fibre optic cable networks that works on this principle. This equipment is commonly used in network testing, monitoring and security, including legal intercepts. These devices often go under the name of passive optical fibre TAP (test access point), fibre splitter, or fibre coupler. In 2024, it was reported that US officials warned cable owners that cables could be vulnerable to tampering by Chinese repair ships.[71]

The challenges around the undersea interception of data have led some analysts to argue that given the vast resources required, and without a clear path to generating usable information, the risk associated with cable tapping remains low and that the efforts of malicious actors would likely be directed toward more accessible targets or use less resource-intensive methods.[72]

Compared with cables located under water, cable landing stations may present a relatively easier target for data interception due to the comparable ease of access on land.[73] The US Office of the Director of National Security classifies the possibility of cyber-attacks on cable landing stations as a 'high-risk' to national security.[74] CLSs are particularly vulnerable to 'insider threat'. As shared facilities, personnel are vetted to varying security levels, and locations in foreign jurisdictions add further complexity.

In particular, Submarine Line Terminal Equipment (SLTE) – which are located within cable landing stations and aggregate massive data flows at a single, fragile junction – may be an attractive target for adversaries who may attempt to compromise optical transport network devices that convert undersea cable signals to terrestrial signals.[75] These systems provide the critical intermediate layer that links SLTEs to data centres and internet service providers. Additionally, the limited number of vendors for SLTE and remote network management systems make them an attractive target for cyber exploitation.[76]

The telecommunications companies that operate cable systems are themselves targets, and access to their broader networks can provide a pathway into the cable systems they manage. Chinese state-sponsored groups such as Salt Typhoon and Volt Typhoon have targeted major telecommunication providers and backbone infrastructure to facilitate large-scale data exfiltration.[77] This included the exploitation of lawful intercept capabilities.[78] US Government assessments indicate that Volt Typhoon's activities are not consistent with traditional cyber espionage operations, like in the case of Salt Typhoon, and assess with high confidence that the group is pre-positioning initial access points ahead of an anticipated conflict.[79]

The primary defence against network tapping is encryption. Encryption can be implemented at the physical layer (Layer 1), higher up in the network communication stack, or across multiple of these layers. In commercially operated submarine cable networks, optical encryption at the physical layer is uncommon, but the functionality is available on some SLTEs on the market. Instead, operators typically prefer to encrypt payloads higher in the stack using protocols including MACsec or IPsec.

Regardless of where the encryption happens, current commonly used methods of asymmetric encryption are vulnerable to the 'harvest now, decrypt later' approach. In this scenario, malicious actors collect and store massive amounts of intercepted data today, waiting for a cryptographically relevant quantum computer capable of breaking it in the future.[80] As this technology matures, sensitive data harvested through state-sponsored espionage campaigns may become accessible, particularly data that transits undersea cables.

Some vendors on the market offer SLTEs that can use keys generated by a separate quantum key distribution (QKD) system. The value of QKD is that any interference with the key exchange is immediately detectable. Some SLTEs also offer post-quantum cryptography (PQC) to secure data in transit, but as quantum repeaters do not yet exist, a 'trusted node' that decrypts and re-encrypts the data must be used over long distances. As such, it is unlikely that any long-haul submarine cable systems have implemented PQC. Data encrypted with traditional protocols therefore remains exposed to harvest now, decrypt later collection.

Border Gateway Protocol (BGP) determines how data packets are routed between networks and misconfigurations can affect both the integrity and confidentiality of transiting data by diverting traffic through unintended networks. This can be intentional (BGP hijacking) or unintentional (BGP leaks). By manipulating BGP route announcements, an adversary could reroute Australian and regional transit internet traffic.[81] China has the capability to reroute international traffic, including undersea cable traffic, towards its surveillance infrastructure through BGP tampering. In 2010, due to a routing leak, China Telecom briefly redirected about 15 per cent of global internet routes for roughly 18 minutes, likely exposing US government and military-related traffic.[82] In 2016, malicious BGP announcements rerouted traffic from Canada to South Korean government websites through China for nearly six months, enabling sustained surveillance. Furthermore, over a two-year period, a China Telecom routing leak via a South Korean peer misdirected global traffic destined for Verizon Asia-Pacific – and notably, for 10 days in 2017, US domestic traffic – through mainland China. Mitigating or detecting stealthy BGP attacks at scale remains difficult.[83] It should be noted that the Internet Engineering Task Force Secure Inter-Domain Routing Operations Working Group is currently working to address the vulnerabilities of BGP.

5.6 Australia's experience

Cable operators often do not publicly report faults, as it could negatively impact their reputation. Faults that take a cable offline mean the service to customers is impacted and the outage requires an operator to move traffic to another route, potentially a competitor's cable. Consultation with several representatives from industry report few repair faults around Australia and island countries in the South Pacific. Publicly reported incidents in recent years include the following.

- In 2021, the container ship *Maersk Surabaya* severed the Australia-Singapore Cable in Perth when its anchor dragged in high winds, which led to legal action against the ship's master.[84]
- In 2022, two of three submarine communications cables between Victoria and Tasmania were accidentally cut on the same day by construction crews working in Victoria and Tasmania. Both unrelated incidents occurred on land.[85]
- In 2025, two Vocus cables off the coast of Western Australia were cut, by what was suspected to be a ship's anchor during cyclonic weather conditions.[86]

The relatively low level of problems with the Australian cables network might be attributed to several factors, including:

- a relatively stable maritime environment (with few earthquakes or volcanic eruptions) with a relatively narrow continental shelf of shallow waters
- a relatively low level of commercial fishing activities conducted near cable locations and shallow water cables
- legislated CPZs in Sydney and Perth that may have discouraged ships anchoring near cables
- Australia's location at a far distance from key areas of geopolitical tension.

It should be noted that significant threats also exist to cables connecting Australia, well beyond waters under Australia's jurisdiction. This is particularly true in choke points such as the Indonesian archipelago (Sunda and Malacca straits – see Figure 19) and the Red Sea, through which the great majority of Australia's westwards-bound data traffic flows. Cable faults occur frequently in the Malacca Strait due to active fishing and cable burial challenges.

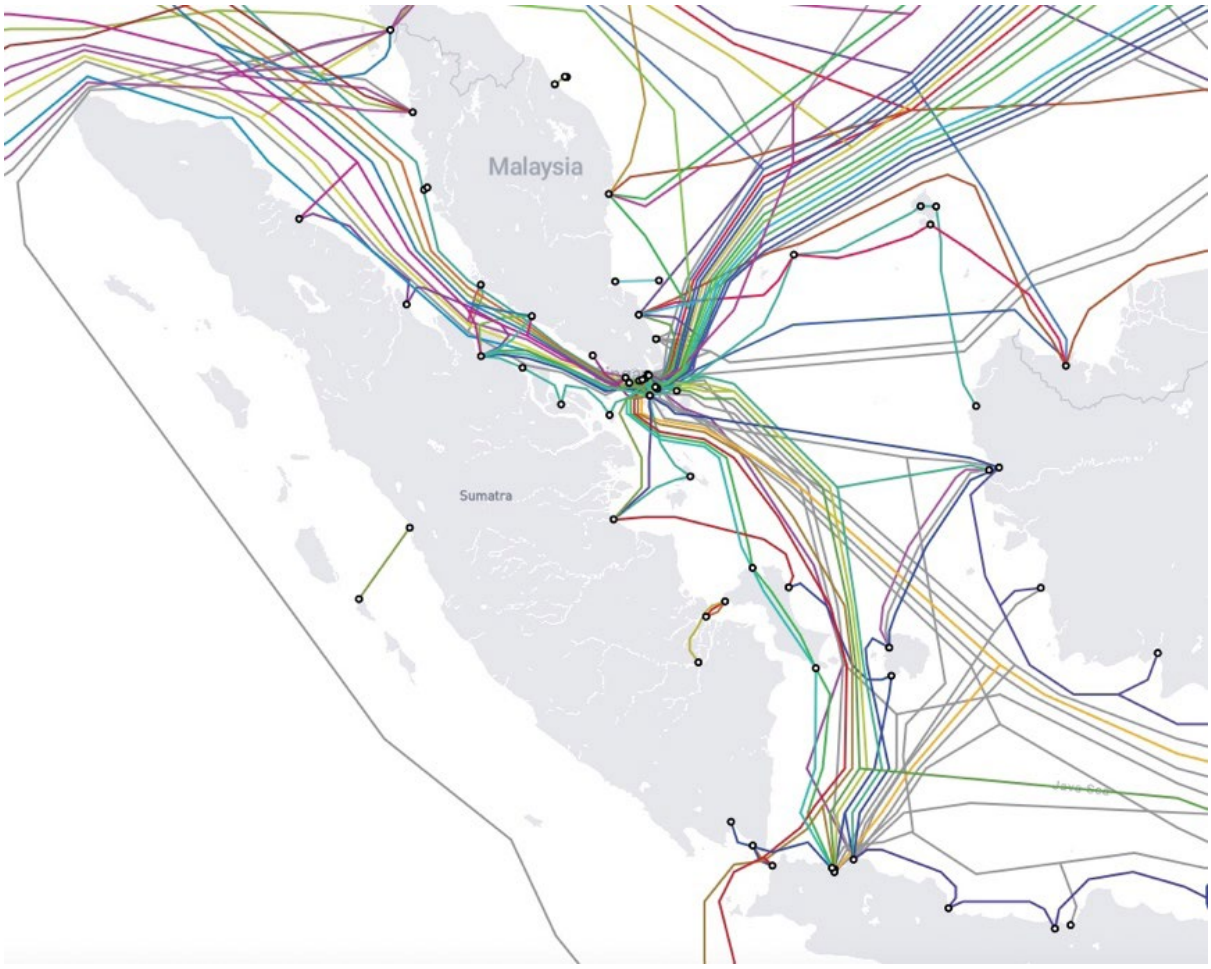


Figure 19: Submarine cables in the Malacca and Sunda straits. Source: TeleGeography.

Recent travel by a Chinese research vessel, *Tan Suo Yi Hao*, along Australia's western and southern coastlines raised concerns. According to the then Australian Opposition Leader, Peter Dutton, mapping of the routes of Australia's cables were one of the likely objectives.[87] Australia's relatively benign peacetime experience is not a reliable guide to future risk. As discussed in Section 5.3, submarine cables have historically been among the first targets in conflicts involving Australia, and the pattern of reconnaissance and probing activity by state actors – including the *Tan Suo Yi Hao* incident – suggests that potential adversaries are actively gathering information about Australia's cable infrastructure. From a defence planning perspective, Australia should assume that its cables would be targeted early in any serious conflict in the Indo-Pacific, and plan accordingly. The relatively low level of incidents to date reflects geography and good fortune as much as effective protection.

Securing submarine cables from disruption or attack

The task of protecting submarine cable systems from interference or attack is an extremely difficult one. A further complication is that primary responsibility for cable security rests with private operators – yet the strategic stakes are too high for government to remain on the sidelines. The result is an evolving and sometimes unclear division of responsibilities between industry and government.

This section discusses ways of enhancing the resilience of Australia's submarine cables to disruption or attack. The integrity of international connectivity cannot be ensured by a single approach, and a range of legislative and non-legislative tools and techniques may be employed to strengthen submarine cable protection measures. It includes the following subsections:

6.1 Enhancing physical resilience of cables

6.2 Use of cable protection zones

6.3 Ensuring NOCs meet Australian jurisdictional and security requirements

6.4 Protection of submarine cables from cyber-attack

6.5 Monitoring and detection of interference

6.6 Routing of cables to avoid high-risk areas

6.7 Effective physical response capabilities

6.1 Enhancing physical resilience of cables

As a starting point, no amount of burial or other protection measures will fully mitigate the risk of damage to cable infrastructure by a motivated deliberate attack. The International Cable Protection Committee (ICPC), in its 2022 paper *Government best practices for protecting and promoting resilience of submarine telecommunications cables*, notes that the industry uses a variety of damage mitigation measures – including route selection, burying, and awareness programs. However, these cannot eliminate all risks. As the ICPC cautions, submarine cables "cannot be hidden or armoured or buried to guard all malicious (or non-malicious) sources of cable damage".[88]

Nevertheless, cable operators are seeking to build resilience through several means including:

- burying cables up to three metres under the seabed in waters down to approximately 1,500 metres, using ploughing or other burial techniques
- improved armouring of cables, especially in shallow waters of less than 500 metres in depth
- improved use of concrete, steel or high-density polyethylene conduits to protect cables close to shore.

These measures can reduce risks of disruption of cables in coastal waters, particularly through inadvertent actions such as fishing or anchoring. Most incidents in Europe and Taiwan have involved ships dragging anchors in shallow waters, whether intentionally or unintentionally. For an intentional attack, this is a simple and inexpensive tactic that also allows for a degree of deniability.

Some physical protection measures, such as burying cables under the seabed, may be more difficult to implement in deep water. At the same time, the disruption of cables in deep water is likely to present some significant challenges for a would-be attacker. One major challenge would be locating the cables. Although the approximate routes of cables can be found on publicly available maps, these may not accurately reflect the location of cables far from shore as cables can move long distances from their original location due to water currents or other factors. There may also be other significant challenges in disrupting cables that may lie thousands of metres below the surface of the ocean.

6.2 Use of cable protection zones

Government regulation can play an important role in stopping vessels from inadvertently damaging cables with anchors and fishing nets. Several states have established CPZs and corridors that prohibit activities that could endanger submarine cables. These geographically defined areas may extend to the limits of national jurisdiction or to water depths beyond which maritime activities pose less of a threat to cable infrastructure.

While CPZs are generally considered to be a useful protection measure, it should be noted that requiring all cables to be laid within protection zones may result in the clustering of cable landings, potentially increasing the risk that a single natural or human-induced incident could damage multiple cables. The geographical extent of protection zones must therefore accommodate the spatial separation requirements of cables where feasible and be appropriately sized.

As discussed in Section 4, Australia has legislated for the creation of several CPZs in Sydney and Perth where fishing, anchoring, and seabed dredging is prohibited, providing incentives for cables to route and land within these zones. Enforcement may, in theory, be carried out via sea or air patrols, with penalties imposed for violations**.** New Zealand has also established several CPZs. Other countries are also actively considering establishing their own CPZs.

It is difficult to definitely prove (in the negative) the utility of CPZs in avoiding incidents. However, it should be noted that to date Australia has experienced only one incident in such a zone, when the container ship *Maersk Surabaya* severed the Australia-Singapore Cable in Perth when its anchor dragged in high winds in 2021. However, Australia's CPZs cover less than half of all international cable landing points in Australia. The expansion of Australia's submarine cable connections, particularly with new cables being landed in Darwin, Victoria, and Queensland, may require the review of the utility of existing legislation and the creation of new zones.

6.3 Ensuring NOCs meet Australian jurisdictional and security requirements

The location of a cable system's primary NOC – the NOC with overall responsibility for the system – is an important security consideration. Most cables landing in Australia currently have primary NOCs located in Australia, but this is not universally the case. As hyperscalers and other large international operators expand respective presences in Australia's cable network, there is a real prospect that primary NOCs for some systems may increasingly be located outside Australian jurisdiction. This matters because NOCs are the nerve centres of cable network management. They monitor system performance, coordinate fault response, and manage network security. Ensuring that these functions are subject to Australian jurisdictional and security requirements – rather than those of another country – is a fundamental aspect of sovereign oversight of critical infrastructure.

US regulators, by means of Network Security Agreements, have been known to require operators to locate either a primary NOC, or secondary NOC that has access to the overall network, on US territory accessible only to US-cleared personnel. Australia should require that operators of cables landing in Australia locate a primary NOC, or a secondary NOC with overall network management capability, within Australia and subject to Australian regulatory authority. There would also need to be a clear understanding of responsibilities between relevant government agencies and NOC operators for threat monitoring, detection and response.

6.4 Protection of submarine cables from cyber-attack

Cyber-attack represents one of the most significant and complex threats to Australia's submarine cable network. As discussed in Section 5.5, the attack surface is broad and spans network management systems, equipment in cable landing stations, wet infrastructure, and cable maintenance vessels. The consequences of a successful attack could range from temporary disruption to permanent physical damage.

Effective cyber protection of submarine cables requires action across several dimensions. First, the supply chain must be secured – ensuring that cable systems are built using trusted equipment and that vulnerabilities are not deliberately introduced during the manufacture or installation of components. The US 'Trusted Network' strategy, which restricts Chinese and Russian involvement in cables connecting with the US, provides a model that Australia has broadly aligned with. Second, cable operators must implement robust cyber security practices across their network architecture and management systems, including network segmentation, access controls, vendor risk management, and software update procedures. Third, government agencies – particularly ASD – must play an active role in working directly with cable operators on threat intelligence sharing and incident response.

Operators can also take other measures to protect against manipulation or exfiltration of data from terrestrial and submarine cables. For example, to protect against 'harvest now, decrypt later' operations, data owners could take a hybrid model approach to their PQC transition, which combines encrypting data in transit using traditional encryption protocols, as well as the new PQC algorithm. This would ensure that even if a malicious actor gains access, decoding that data would be significantly more difficult.[89]

Addressing these challenges comprehensively requires a coordinated national approach. The cyber security measures that should form part of Australia's national submarine cable strategy are set out in Section 9 and represent some of the most urgent actions Australia needs to take.

6.5 Monitoring and detection of interference

Monitoring and detection of interference in submarine cables is a key first step to an effective response by cable operators and maritime enforcement agencies. However, this can be an extraordinarily difficult endeavour due to several factors.

- Distance: cables may run for thousands of kilometres in remote waters.
- Undersea: cables may be thousands of meters below sea level.
- Jurisdiction: cables will often pass through multiple national jurisdictions (including territorial waters and EEZs) and international waters, meaning no country has sole overall responsibility.
- Private operators: the great majority of submarine cables are privately owned and operated, meaning private companies will often be better placed to take principal responsibility for monitoring and detection of interference.

Some cable operators have implemented surveillance systems based on AIS transponders carried by large commercial vessels to detect ships loitering or anchoring near cables. AIS data gathered by numerous maritime authorities can be integrated into cable operator NOC information systems to give real-time situational awareness of vessel traffic and potential threats to submarine infrastructure. Integrating AIS into NOC monitoring systems is only as effective as the ability of NOC personnel to directly or indirectly (via Navy or Coast Guard) contact vessels that may pose a threat to submarine cable integrity.

In some high-risk areas with substantial maritime traffic, such as Singapore, cable operators have proven the benefit of AIS coupled with direct vessel contact to avoid accidental anchor damage. However, these systems rely on vessels advertising respective locations using AIS devices and so will only likely be effective in preventing inadvertent/negligent activities in shallow waters and not intentional attacks. Further, in Australia, there is no clear understanding between private operators and maritime law enforcement agencies as to responsibilities for communicating and engaging with vessels that are deemed to be a potential threat.

Some cable operators are advocating and actively implementing new cable protection technologies to enhance monitoring of maritime vessel traffic that may pose a risk to

submarine cable infrastructure. Distributed Acoustic Sensing (DAS) technology has been applied to several cables in Australia. DAS technology utilises a dedicated optical fibre in the cable system that acts as a sensor to detect vibrations, strain and temperature changes. This is achieved by transmitting laser pulses down the optical fibre and analysing backscattered light that is altered by external mechanical stress from events such as passing maritime vessels, seismic activity or underwater impact events from fishing activities and vessel anchoring. DAS allows for real-time monitoring of the submarine cable environment to enable early detection of threats before possible damage occurs.

However, DAS has detection limitations related to the distance along the optical fibre from the DAS equipment, typically installed in the cable's CLS. It can currently only be used for one or two repeater spans (up to around 100-200 kilometres) and not the entire length of a long cable. However, as this technology develops, effective detection lengths are readily increasing. For new cable systems, the dedicated optical fibre path design can be optimised to pass through one or more optical amplifiers to extend the effective reach of DAS to a few hundreds of kilometres.

DAS technology can be retrofitted to existing submarine cables, but only where a spare optical fibre is available, or can be incorporated into new cable system design without requiring a dedicated optical fibre. Monitoring of DAS information is performed by the cable operator's NOC personnel. DAS information must be complemented by NOC personnel contacting maritime vessels in real-time to warn they may pose a threat to the submarine cable system.

Combining DAS with other new subsea fibre-sensing technologies offers a potentially transformative opportunity in the protection and use of submarine cables. They can be simultaneously used to defend cables against accidental, negligent, and malicious damage while offering a persistent maritime domain awareness function. Fiber-sensing technologies including Coherent Optical Frequency Domain Reflectometry and State of Polarisation sensing may be combined with DAS and artificial intelligence and machine learning to interpret underwater objects and events. Machine learning trained on acoustic signatures can detect vessel movements, classify vessel types, track maritime traffic, and identify unusual seabed activities. Such systems could potentially provide a range in excess of 150 kilometres, metre-level spatial resolution, and co-existence with live data traffic.

6.6 Routing of cables to avoid high-risk areas

Perceived threats are also impacting the routing of new cables. As far as possible, the routing of new cables will avoid shallow water, areas where environmental risks such as earthquakes or other geological movement exist, or risky human activities such as intensive fishing.

Cable operators are also paying much more attention to geopolitical risks in planning routes to potentially avoid maritime choke points such as the Malacca or Sunda straits, where cables could be easily disrupted, or in areas of disputed jurisdiction. For example, many operators are now seeking to avoid laying new cables in much of the South China Sea due to concerns about jurisdictional claims from China and other countries, and the potential for interference. Meta's Project Waterworth cable, a planned 50,000-kilometre cable circling the globe, will avoid the Red Sea, Malacca Strait, and the South China Sea (see Figure 20). According to public reports, it will also be laid as much as possible in deep waters with the cables buried under the seabed in high-risk fault areas.[90] Other recently announced new cables connecting with Australia, such as Google's Dhivaru Cable across the northern Indian Ocean[91] and the Talaylink cable between Thailand and Australia[92] do not transit the Malacca Strait to Singapore as is usually the case. Neither will Inligo Networks' Asia Connect Cable System (ACC-1) which will link Darwin to Southeast Asia, Guam, and North America.

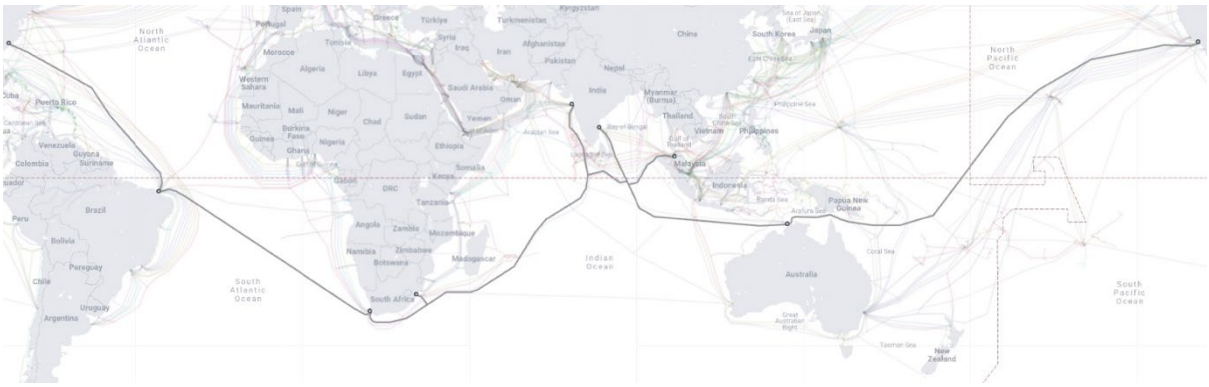


Figure 20: Routing of Meta's planned Project Waterworth cable. Source: TeleGeography.

These new cable routes have the potential to reduce the risk of physical attacks on cables that may be bunched in shallow-water maritime choke points. Australia could also benefit from these developments by becoming a hub for cables transiting the Indo-Pacific, which would increase and diversify its cable connectivity.

6.7 Effective physical response capabilities

Ultimately, the ability to deter or address attacks on cables depends on the existence of effective response capabilities. This requires a clear understanding of roles and responsibilities among relevant security agencies and between government agencies and private operators, clear doctrine governing how to respond to various types of threats, and the necessary capabilities to act on that doctrine. In our view, Australia is currently poorly served in all these respects. The following discusses the two principal agencies with response responsibilities – the ADF and MBC – and identifies key gaps that need to be addressed.

The ADF holds primary responsibility for securing the undersea domain – including commercial cable networks and Defence-owned subsea infrastructure – and conducting undersea and seabed warfare in respect of state-based adversaries, exercising the defence powers of the Commonwealth. State actors possess a range of capabilities that could be used to interfere with cable infrastructure, from conventional submarines and combat divers to UUVs. Evidence from European incidents and open-source reporting suggests that adversaries are actively using such capabilities for reconnaissance of cable routes and seabed infrastructure. ASW capabilities and counter-UUV development are both directly relevant to cable protection. Australia should ensure that the protection of submarine cable infrastructure is explicitly considered within its ASW and counter-UUV planning – including within the AUKUS advanced capabilities pillar – alongside more traditional submarine warfare priorities.

The ADF is now giving much greater focus to building capabilities for undersea and seabed warfare. In April 2026, the Royal Australian Navy announced the establishment of a Maritime Autonomous Systems Unit (MASU), which is a specialised unit dedicated to integrating, operating, and deploying uncrewed maritime systems. MASU will operate a mix of autonomous systems, including the *Ghost Shark* (see Figure 21) extra-large autonomous underwater vehicle, the *Bluebottle* uncrewed surface vessel, and the *Speartooth* large uncrewed underwater vehicle.[93] All of these may be relevant to monitoring cable systems and, potentially, responding to attempted disruptions.

Figure 21: Deputy Prime Minister and Minister for Defence, the Hon Richard Marles MP and Minister for Defence Industry and Minister for Pacific Island Affairs the Hon. Pat Conroy MP announcing the contract with Anduril Australia to acquire a new fleet of Australian designed and built extra-large autonomous undersea vehicle – known as the Ghost Shark – for the Royal Australian Navy, at Fleet Base East in Sydney, 2025. Source: Australian Department of Defence.

The strategic significance of these capabilities was underscored at the 2026 Shangri-La Dialogue in Singapore, where Defence Minister Richard Marles described the seabed as having become "a major field of contest" and warned that the pattern of cable cutting incidents in the Baltic and around Taiwan may indicate that adversaries are "testing our response times, testing our attribution thresholds and testing our political will to respond".[94] On the sidelines of the Dialogue, Marles joined US Defense Secretary Pete Hegseth and UK Defence Secretary John Healey to announce a new AUKUS Pillar II project to develop advanced weapons systems and sensors for underwater drones, with delivery to war fighters expected from 2027. The three leaders explicitly identified the protection of undersea cables as among the project's core objectives. This announcement represents a significant step in translating Australia's stated commitment to cable protection into concrete capability development.

In addition to general naval capabilities, the ADF also has specialist capabilities relevant to submarine cables. In 2023, the ADF acquired the Norwegian flagged MV *Normand Jarl* for A$110 million, which was recommissioned as an auxiliary support ship, ADV *Guidance* (see Figure 22). This ship displaces 7,400 tons and is 107 metres long and 22 metres wide with a large cargo deck and a crane. According to Navy, the primary role of ADV *Guidance* is to support undersea surveillance systems trials, including the ability to deploy undersea crewed and uncrewed vehicles, and robotic and autonomous systems.[95] With necessary resourcing, the ADV *Guidance* could play a valuable role in enhancing Australia's ability to monitor submarine cables and other critical subsea infrastructure.[96] As will be discussed in Section 7, there may be options for the Australian Government to acquire cable repair equipment (e.g. cable drums, test equipment, etc) that could be stored onshore and fitted on the ADV *Guidance* in the event of a contingency.

Figure 22: Undersea Support Vessel ADV Guidance at Eden, New South Wales, as part of Exercise Dugong 24. Source: Australian Department of Defence.

Clearance diving and mine countermeasures are also relevant. In some circumstances (specifically in shallow waters) clearance divers can have a direct role in inspecting cable infrastructure for signs of tampering, attached devices, or damage. Mine countermeasure capabilities – including sonar systems, remotely operated vehicles, and mine countermeasure vessels – may also be needed to detect and neutralise devices placed on or near cables. Australia's mine countermeasures capability has historically been limited and represents an acknowledged gap in the country's overall maritime capability. As the threat environment evolves and state actors demonstrate both the intent and means to interfere with seabed infrastructure, there is a strong case for ensuring that clearance diving and mine countermeasure assets are adequately resourced, and that their potential role in protecting cable infrastructure is explicitly recognised in relevant ADF operational planning.

Another vital element is MBC, a command within the ABF with responsibility for monitoring, detection and response to a range of civil maritime threats. It is commanded by a Navy Rear Admiral and has access to maritime capabilities within the ABF as well as capabilities specifically tasked from Navy. MBC's status as a civil maritime law enforcement agency gives it an important role in providing non-escalatory response options to cable incidents, particularly in ambiguous cases where attribution is uncertain. MBC would be supported by the ADF, ABF, DFAT, Home Affairs, ACMA, and federal and state police forces.

The boundary between civil and military responses to cable threats may be less sharp in Australia than in other countries, given MBC's leading role in civil maritime law enforcement. While this is an advantage, it requires clear doctrine governing when and how ADF capabilities are brought to bear in response to cable incidents. Developing such doctrine should be an explicit element of any national submarine cable strategy.

Together, the ADF and MBC provide the foundation for an effective response capability to threats against Australia's submarine cables. However, realising that potential requires clearer doctrine, better resourcing, and more explicit integration of cable protection into operational planning. These are not merely administrative matters, but are prerequisites for credible deterrence. An adversary that doubts Australia's ability to detect and respond to cable interference is an adversary more likely to attempt it.

Repair and maintenance

Access to prompt and efficient repair and maintenance of submarine cables that connect with Australia is a major factor in recovering from physical disruptions to the country's submarine cable network. Around the world, arrangements for the repair and maintenance of Australia's cables are currently within the control of private operators that have banded together into regional 'clubs' to contract with private service suppliers. Governments have little or no input into decisions about the repair of privately owned infrastructure, including the prioritisation of repairs.

These existing arrangements appear to be adequate for 'normal' times where disruptions to cables are overwhelmingly caused by inadvertent human activities such as fishing, anchoring, or environmental causes.[97] However, the potential for intentional disruption, particularly state-based attacks on multiple cables, would place a severe strain on this 'business as usual' approach.

This section discusses existing arrangements for the maintenance and repair of Australia's submarine cables, as well as options to enhance sovereign capabilities in maintenance and repair. It has the following subsections:

7.1 Global repair numbers

7.2 Current maintenance and repair arrangements for Australian cables

7.3 Options for enhanced maintenance and repair arrangements

7.1 Global repair numbers

Submarine cable faults arise from a variety of sources, with both human activities and natural events contributing significantly to disruptions. Most faults are due to what the industry calls 'external aggression', primarily from fishing trawlers and ship anchors inadvertently damaging cables on the seabed. As noted previously, natural phenomena such as earthquakes and underwater landslides account for roughly 7 per cent of incidents, while equipment malfunctions represent around 3 per cent, with the remainder being the result of human activities.

According to the ICPC, on average approximately 190 cable repairs occur each year globally, with some 178 repairs made in 2025.[98] In recent years, repair numbers have remained relatively stable despite a significant increase in the number of in-service cable kilometres, with the fault rate decreasing from one fault per 5,173 cable km in 2015 to one fault per 10,569 cable km in 2025. Further, in 2025, 43 per cent of all cable repairs were made in international waters, 55 per cent in EEZ waters, and 2 per cent in territorial waters.

According to ICPC data, the average time globally between an operator reporting a fault and commencement of repairs was 49 days, down from 2022, but still considerably higher than previous years. Repair frequency in Asia and the Middle East exceeds that of all other regions combined. Figure 23 shows global data on time between fault reporting and repair commencement for EEZ and territorial seas in 2025. It shows that times for cables located in Australian territorial waters/EEZ are middle of the range, but repair times in waters north of Australia are considerably longer.

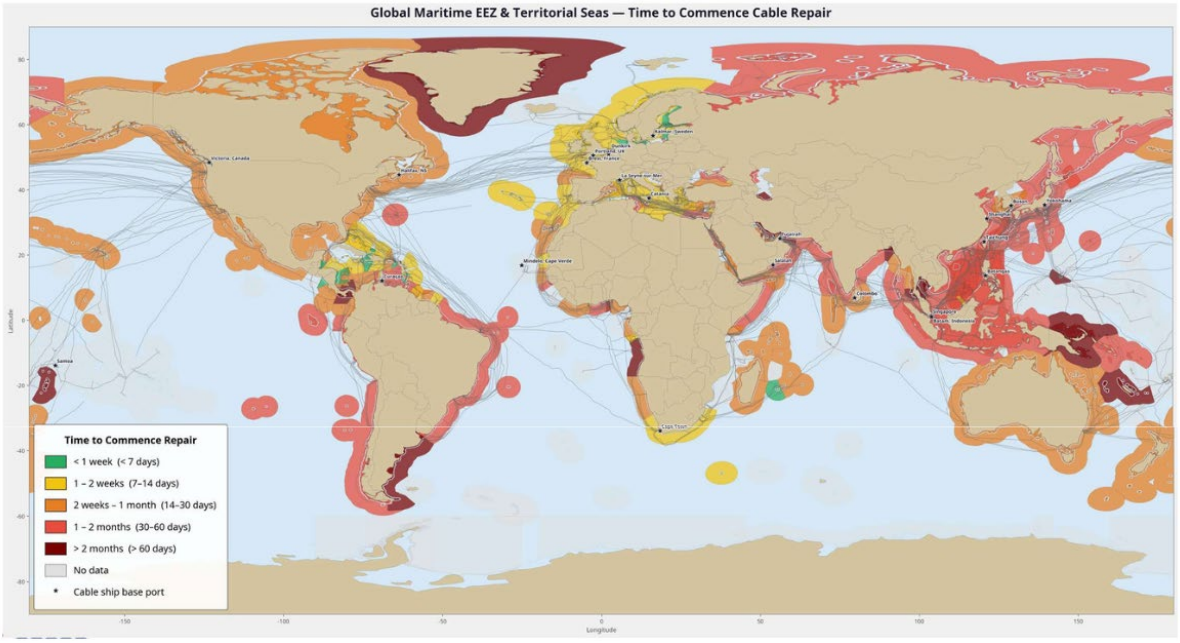


Figure 23: Time to commence cable repair – Global maritime EEZ and Territorial Seas, 2025. Source: ICPC

7.2 Current maintenance and repair arrangements for Australian cables

Given the complexity and criticality of submarine cable networks, the submarine cable industry relies on comprehensive maintenance agreements to ensure timely and effective repairs when submarine cable faults or damage occurs. Maintenance agreements are formal contracts between cable owners and specialist maintenance providers. Their primary purpose is to establish a framework for rapid response and repair of submarine cables, minimising downtime and disruption.

Maintenance agreements are based on a cost-sharing model and regional geographies. Multiple cable owners share the cost of having specialist cable repair vessels and specialist equipment stationed in-region at defined base port locations within the respective agreement zone or boundaries. Annual fixed fees allow maintenance providers to dedicate the vessel and cable storage depot assets described above to maintenance duties. In the event of a cable fault, the cable owner(s) notifies the provider, who then mobilises the cable repair ship to the fault location. A variable fee is charged for each repair operation to cover the operational costs of the cable repair vessel. Ensuring capabilities to quickly repair damaged cables is increasingly a key focus for operators and policymakers.

Repair contracts typically provide for an annual fixed fee based on the number of kilometres of cable that is located within the zone boundaries. Additional fees are charged for spare cable storage in depots located close to or in the same location as the repair ship base port. There are generally no specific contractual arrangements for prioritisation of repairs where multiple cables need repair (other than a first-come first-serve basis), although operators often informally cooperate among themselves to allow high-priority or service-affecting repairs to be undertaken first. Importantly, national governments have no input on prioritisation of repairs, even in cases of national emergency.

These contractual arrangements are designed to provide adequate repair capabilities for ‘business as usual’ conditions, involving repair of cables required due to internal faults, environmental disruption, or human activities. These arrangements are being put under some commercial pressure due to the rapid expansion of international cable networks, particularly by the hyperscalers, which may have the market power to alter existing arrangements.

Further, existing arrangements were not designed to properly respond to major conflicts that may involve the cutting of multiple cables. Repair vessels may also find it difficult to operate in conflict zones without naval escorts or special arrangements relating to crew protection and insurance. This is particularly relevant to the recent spate of cable faults and subsequent repairs in the Red Sea, where repair vessel operators needed to coordinate closely with naval authorities to ensure adequate security and protection.

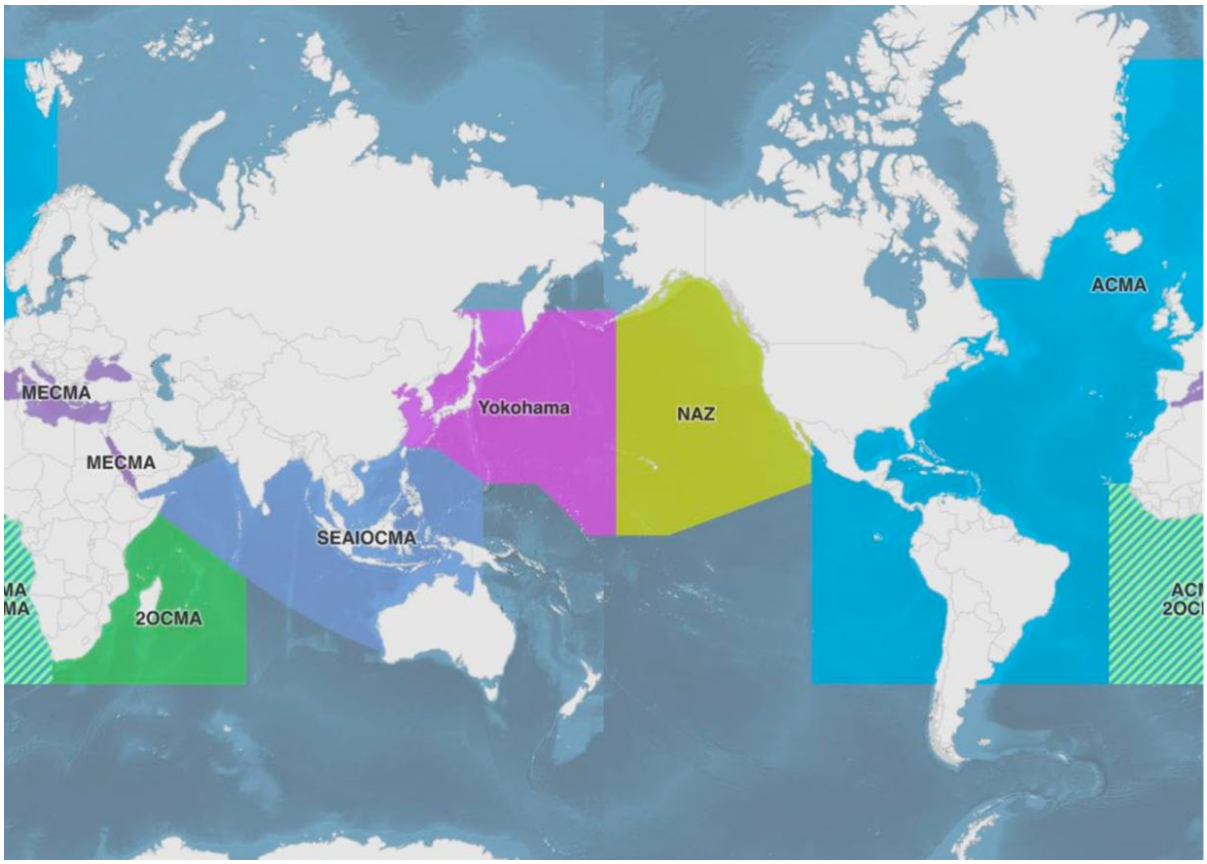


Figure 24: Maintenance agreement zone boundaries worldwide – consortium. Source: TeleGeography, Infra-Analytics.

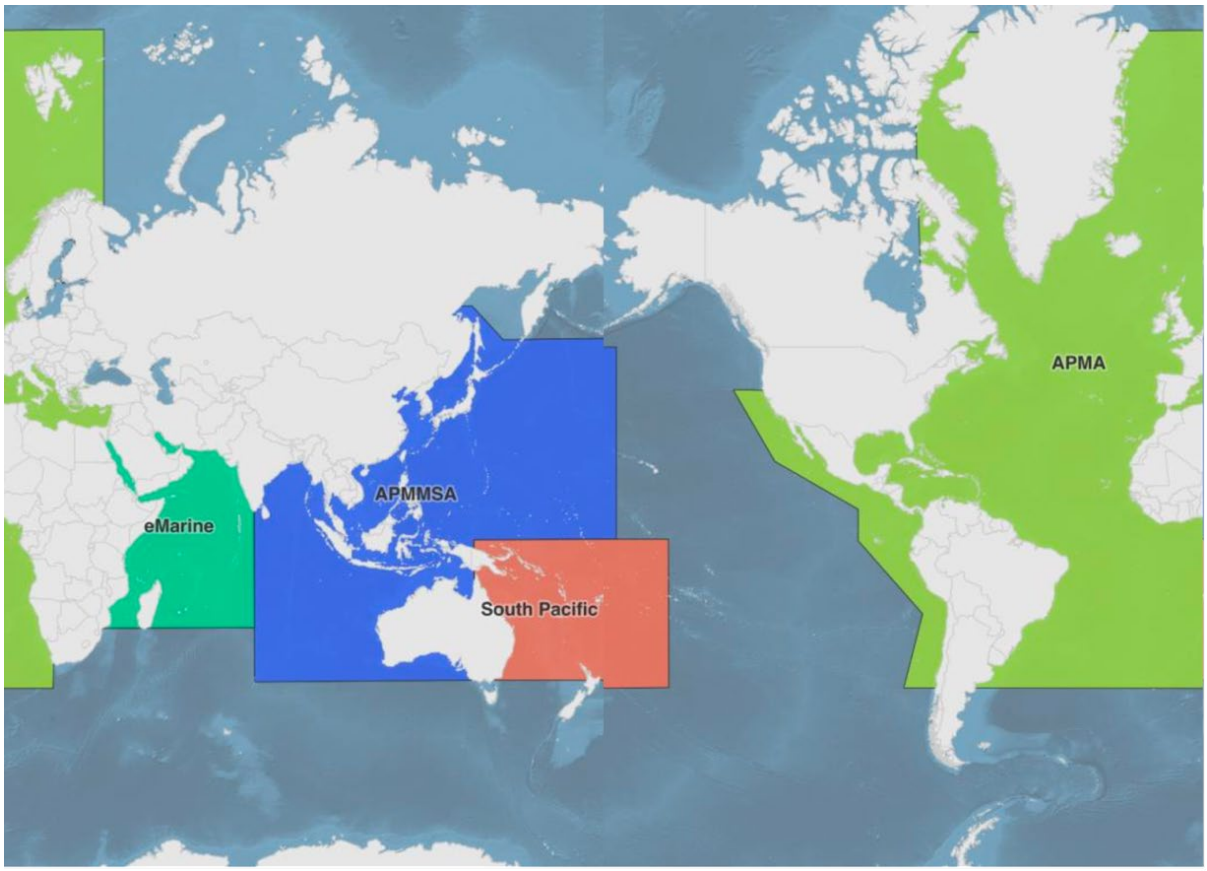


Figure 25: Maintenance agreement zone boundaries worldwide – private. Source: TeleGeography, Infra-Analytics

As shown in Figures 24 and 25, the waters adjacent to Australia are covered by three maintenance agreements. Cable repair vessels are stationed at base ports within each agreement's boundaries and compete to secure five-year contract commitments from cable owners for cable maintenance services.

- ***South Pacific Marine Maintenance Agreement (SPMMA)*** (private arrangement). One cable repair ship is allocated to the SPMMA agreement, which is stationed in Suva, Fiji and operated by Optic Marine Services (OMS) headquartered in Malaysia. This zone has approximately 100,000 kilometres of cable within its boundaries.
- ***South East Asian Indian Ocean Cable Maintenance Agreement (SEAIOCMA)*** (consortium arrangement). Four cable repair ships based in Singapore and Sri Lanka support the SEAIOCMA agreement; including three ships contracted for 12 months of the year and one for three months per year. They are operated by ASEAN Cableship[99] and Global Marine.[100] SEAIOCMA repair vessels that maintain approximately 135,000 kilometres of cable are the most highly utilised in the world due to high repair rates, primarily in the South China Sea. This pressure results in frequent queues for repairs and long repair wait times.
- ***Asia Pacific Marine Maintenance Agreement (APMMSA)***. Three cable repair vessels support repairs in this zone and are stationed in Taiwan and Indonesia. They are operated by Alcatel Submarine Networks (ASN), headquartered in France, and OMS. As this is a private maintenance agreement, repair vessels can undertake non-repair activities, meaning they are not dedicated full-time to repair operations. Industry estimates indicated that approximately 85,000 kilometres of cable are covered by this agreement.

At least some of these maintenance arrangements also include operators of submarine power cables.

It is notable that cable repair vessels that cover cables landing in Australia are stationed considerable distances away. Spares depots are also located at considerable distances from Australia. All cable repair vessels are also operated by foreign companies with mostly foreign crews. While these arrangements do not now involve Chinese-operated cable repair vessels, the Australian Government may not currently have the authority to prevent that from occurring.

Existing repair arrangements may well be adequate for 'business as usual' conditions, but they would be clearly inadequate in dealing with concerted state-based attacks against Australia's cable network. The Australian Government does not currently have any way of ensuring that repairs would be undertaken in a timely manner by trusted service providers or that repairs to key cable systems are prioritised.

7.3 Options for enhanced maintenance and repair arrangements

There are several approaches that could give Australia more options for repairing cables in the case of conflict or national emergency. Developing sovereign capabilities may be expensive, with new cable repair vessels costing approximately US$150 million to build and equip. Ensuring timely access to spares also comes at significant cost. Even more importantly, Australia does not have the necessary expertise to operate specialist repair vessels. Other nations have such industries. Countries such as France, the UK, and Japan have privately owned operators in the cable production, installation, or repair industries. This dynamic can be used to provide those governments with national capabilities that could potentially be mobilised in the event of a conflict.

In 2024, France bought back control of submarine cable company ASN, which can manufacture, lay, and repair cables.[101] In 2025, a UK parliamentary inquiry recommended the acquisition of a national repair ship and Royal Navy crews trained for cable repair.[102] India is also exploring whether to subsidise Indian companies to build an Indian-controlled repair ship or convert navy ships for the task.[103] Indian risk assessments identified that the country also relies on cable repair vessels stationed considerable distances away and are operated by foreign entities with foreign crews. The US, by contrast, has moved the other way by defunding its Cable Security Fleet, although the US Government does charter at least one maintenance vessel, presumably to service military cables.

Options for enhanced maintenance and repair arrangements that could be considered by the Australian Government include the following.

- ***Enhancing Navy capabilities:*** enhancing existing Royal Australian Navy capabilities in this domain, including contingency options for fitting cable maintenance/repair capabilities on the ADV *Guidance.* It may be possible for the Australian Government to acquire necessary repair equipment that, in a contingency, could be fitted on the ADV *Guidance* in a relatively short time frame.
- ***Strategic Fleet capability:*** acquiring a cable maintenance/repair vessel through a public-private partnership, potentially as part of Australia's Strategic Fleet.[104] This could, for example, include refitting an offshore service vessel used in the offshore oil and gas industry, that would be operated by an Australian company under an Australian flag and with an Australian crew. The Australian Government would retain the right to 'call in' the vessel in times of national emergency.
- ***Shared capabilities with international partners:*** shared access to sovereign capabilities along with one or more of Australia's key international partners (e.g. the US, Japan, India, or a European country). This approach would raise issues regarding the location of vessels and prioritisation of repairs.

- ***Priority access arrangement with private provider:*** entering into contractual arrangements with an existing commercial service provider in a maintenance zone adjoining Australian waters under which the Australian Government could gain priority access to repair services for a fee. This would require amendments to existing agreements to prioritise repair operations, requiring the agreement of all counterparties (cable owners and repair vessel operators).

All these options would involve finding a balance between an adequate degree of sovereign control over repair arrangements and ongoing costs to Australian taxpayers.

Most options for enhanced sovereign repair arrangements would also need to consider several other factors.

- ***Timely access to spares:*** spares for Australia's cable systems are currently located in depots at considerable distances from Australia. Any enhanced repair arrangements would need to include timely access to spares. This may involve a requirement that private operators locate a portion of spare parts for their systems within Australia.

- ***Access to specialised workforce***: Australia's reliance on foreign maintenance providers has resulted in a significant shortage of skilled workers in Australia. Any sovereign repair arrangements would necessarily need to address requirements for local training and expertise in cable repairs. One of the key recommendations of a recent UK parliamentary inquiry included the training of reserve officers in cable repairs and this may be something the Royal Australian Navy should also consider.

- ***Protection of cable repair ships:*** a further consideration is the need to protect (and insure) repair vessels themselves during conflict or heightened tension. As has been seen in the Red Sea in recent times, cable repair operations in contested waters may require close coordination with naval authorities. Australia should consider what arrangements would be needed to support and protect repair operations in Australian waters or adjacent areas during a conflict or crisis, including potential exercises involving protection of repair vessels.

Existing arrangements for the repair and maintenance of Australia's submarine cables were designed for peacetime conditions and are adequate for the routine faults that characterise normal operations. They were not designed to respond to the deliberate and coordinated attacks on multiple cables that a state-based adversary might conduct. Australia currently has no guaranteed access to trusted repair capabilities in a national emergency, no sovereign repair vessel(s), and no stockpile of spares located within Australian territory. Addressing these gaps will require a combination of enhanced naval capabilities, public-private partnerships, and international cooperation with trusted partners. The options set out in this section are not mutually exclusive: a layered approach that combines several of them is likely to be more resilient than reliance on any single arrangement. Getting this right is an essential element of any credible national submarine cable strategy.

Working with industry and international partners

This section discusses the imperatives and dynamics of working with industry and international partners to enhance the resilience of Australia's cable network. This section contains the following subsections:

8.1 Working with Australian industry partners

8.2 Working with international multilateral groupings

8.3 Working with Quad and AUKUS partners in the Indo-Pacific

8.4 Working with European partners

8.5 Engagement with Pacific partners

8.6 Engagement with Indian Ocean partners

8.7 Engagement with partners in Southeast Asia

Currently, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCSA) has a leading role in regulating and working with private cable operators. DFAT, through the Cable Connectivity and Resilience Centre, plays a leading role in international engagement, including with international organisations, regional partners, and industry forums.

8.1 Working with Australian industry partners

The government-private interface creates one of the most significant challenges in protecting submarine cables. Submarine cables were once largely the preserve of mostly state-owned telecommunications companies. However, beginning in the 1990s, nearly all submarine cables became privately owned and operated, whether by telecommunications companies, specialised operators, and now, by the hyperscaler technology companies.

Privately owned infrastructure that has long been only lightly regulated has now become critical to the national security of Australia and many other countries. Cooperation between government and industry is fundamental to building resilience in the global network, but also in the Indo-Pacific. Governments need to understand first-hand the issues and challenges facing the submarine cable industry, including across all facets of the ecosystem, from investment challenges, to licencing and permits, to supply chain constraints and cable repair challenges.

The ability of the Australian Government to control – or even influence – decisions by private operators in respect of issues such as cable design (e.g. secure-by-design or monitoring technology), routing/landing decisions or repair arrangements, is currently limited. While ACMA, the principal Australian regulatory agency in respect of submarine cables, regularly consults with industry, its regulatory authority on many issues affecting security is quite constrained. Broadening cables industry consultation mechanisms beyond ACMA would be an important step. Key agencies with responsibilities in this space, such as MBC and ASD, do not have formal mechanisms for liaison with cable operators and nor is there a clear understanding of responsibilities in relation to detection or response to threats as between private operators and government agencies.

Without formal liaison mechanisms, government agencies risk being perpetually reactive, responding to incidents after the fact rather than working with operators to build shared situational awareness and response capabilities. The appointment of specified liaison officers by those agencies could be a useful step in getting ahead of the curve in terms of risk mitigation and response. However, a broader review of the government-industry relationship may be required, including the scope of current regulatory authority.

8.2 Working with international multilateral groupings

Australia is an active player in international groupings that bring together submarine cable industry representatives and governments to discuss issues of common interest. Recently, there has been an increased focus on ways of enhancing network resilience.

The ICPC was established in 1958 to promote the protection of submarine cables and represent the industry's interests with national government regulators and international institutions such as the United Nations. The ICPC comprises members from all parts of the submarine cable ecosystem including owners, operators, system suppliers, seabed users, maintenance vessel operators, and a range of government members. It now includes some 243 members, including the Australian Government through DFAT (the first government in the world to join) as well as eight Australian operators and other organisations.

In 2022, the ICPC adopted a document titled *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*.[105] This guide provides an important resource for governments and operators to build and operate cables in a manner that mitigates threats.

Regional associations have also been formed that coordinate with the ICPC and act as forums for dialogue and collaboration within the industry and with government and other stakeholders relating to region-specific issues. There are regional cable industry associations in Europe (the European Subsea Cables Association), and the US (the North American Submarine Cable Association). However, no industry association has been established in Southeast Asia or the Oceanic region. It would be in Australia's interests for an Asian/Indo-Pacific regional cable industry association to be established to coordinate regional initiatives.

Australia also engages with international partners from government and industry through the International Telecommunication Union's International Advisory Body on Submarine Cable Resilience, which was established in 2024. Australia is represented on that body through DFAT's Cable Connectivity and Resilience Centre. The body's February 2026 meeting adopted a declaration as well as recommendations in the following areas:[106]

- timely deployment and repair (including streamlining of regulatory processes; strengthening global repair architecture and public-private partnerships)
- risk identification, monitoring and mitigation
- fostering connectivity and geographic diversity.

8.3 Working with Quad and AUKUS partners in the Indo-Pacific

Groupings such as the Quad, AUKUS, and similar mini-lateral arrangements could provide useful frameworks for Australia to work with key security partners regarding submarine cables.

In 2018, Australia joined a trilateral partnership with the US and Japan[107] (as well as other trusted partners) to fund several cable projects in the Pacific that otherwise may have been built by Chinese firms. These include the East Micronesia Cable System (US$95 million funded by Australia, the US, and Japan), the Palau ECHO Submarine Cable Branch System (US$30 million, funded by Australia, the US, and Japan); and the Tuvalu Vaka Cable (funded by Australia, the US, Japan, New Zealand, and Taiwan).[108]

The Quad provides a useful framework for Australia to work with India, in addition to the US and Japan, in enhancing the resilience of cable networks in the Indo-Pacific. In 2023, the Quad partners launched the Quad Partnership for Cable Connectivity and Resilience, which involves a shared commitment to enhance submarine cables as a priority regional infrastructure. Although not fully publicly acknowledged, a key objective of the

initiative is to limit China's influence in regional telecommunications infrastructure, including through assisting in the development of cable connectivity in the region on attractive terms. The Quad initiative also prompted Australia to establish its Cable Connectivity and Resilience Centre within DFAT to enhance technical support, policy, and repair capabilities in the region.

AUKUS also has direct relevance to the protection of Australia's submarine cable infrastructure. The AUKUS advanced capabilities pillar, which among other areas covers undersea capabilities, autonomous systems, and electronic warfare, provides a framework for Australia to develop and share capabilities directly applicable to seabed domain awareness and cable protection. Australia should ensure that cable infrastructure protection is explicitly considered within relevant AUKUS workstreams, particularly those relating to undersea surveillance and counter-UUV capabilities.

8.4 Working with European partners

Australia could also benefit significantly from stepped-up engagement with European partners in submarine cable policy. Although geographically not within the Indo-Pacific (except for France), European countries could be highly valuable partners in Australia's efforts to protect its submarine cable network. The numerous incidents that have occurred involving submarine cables in northern European waters since 2022 have prompted the EU and NATO to significantly enhance surveillance and response capabilities.

There are a number of recent European and NATO initiatives that may be of interest to Australia.

- In 2022, the French Ministry of Armed Forces released a national *Seabed Warfare Strategy* that focuses on securing, monitoring, and controlling undersea infrastructure to ensure digital sovereignty, national security, and economic interests (see Section 9).
- The EU adopted an *Action Plan on Cable Security* (2025) and a *Cable Security Toolbox* (2026) that provides a set of mitigating measures against identified threats/vulnerabilities/dependencies and proposes a list of new strategic cable projects with public funding and proposals for maintenance and repair arrangements (see Section 9).
- In 2024, NATO established a Critical Undersea Infrastructure Network to improve information sharing and coordination for the security of undersea cables and pipelines, which brings together stakeholders from allies' governments, industries, NATO's civilian and military headquarters, as well as other relevant actors. Although its initial focus was on the Baltic Sea, it has since expanded its focus to the Mediterranean.
- NATO also established a new Maritime Centre for the Security of Critical Undersea Infrastructure, based in the UK.
- NATO has also launched its HEIST (Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications) project, which aims to develop strategies to protect global internet traffic and create alternative pathways in case the global undersea cable network becomes compromised. According to NATO, HEIST will result in augmented threat detection, fault diagnosis, and communication resilience for submarine cables.[109]

Australian submarine cable initiatives in the Pacific

Dr Amanda H A Watson, Australian National University

The Australian Government has been actively engaged in supporting Pacific Island governments with the development of undersea cable infrastructure in recent years. The Coral Sea Cable System (CS2) for PNG and Solomon Islands, which was completed and officially launched in 2019, was the first of a suite of cable projects. Australia's second cable-related announcement was a second cable for Palau, to be jointly funded with Japan and the US. These two projects signalled approaches Australia would continue to adopt: operating on its own in some cases, such as with CS2, and acting jointly with fellow donor partners in other instances.

In annual forum communiques and other official communications, the Pacific Islands Forum has highlighted digital connectivity of Pacific member states as a central goal, alongside a need to ensure cyber security.[110] To help meet connectivity ambitions, Australia has been providing cables to Pacific countries not previously connected, including Kiribati, Nauru, and Tuvalu, and providing a second cable to countries with just one cable, such as Palau, Solomon Islands, and Tonga.

Australia's cable efforts cross multiple federal government departments and are facilitated by the AIFFP. The Cable Connectivity and Resilience Centre aims to coordinate efforts across departments, as well as with fellow donors and other stakeholders.

In coming years, assessments will be made as to whether Australia's cable strategy in the Pacific has been successful. Some may argue that undersea communication cables are becoming obsolete because of new LEO satellite technologies. However, cables enable substantial bandwidth to enter an area and are generally reliable, although cable breaks occur due to varied causes.[111] Given that the Pacific region is aiming for improved connectivity,[112] Pacific leaders are unlikely to be concerned about the specific technology (or technologies) utilised to achieve the intended outcomes.

Further investigation could assess whether cable deployment has led to decreases in consumer internet prices, given that potential decreases have been mentioned in project announcements.[113] In the case of CS2, prices were unchanged in PNG for more than two years after the official launch.[114] Subsequent price decreases occurred at the time when a new mobile operator entered the market[115] and it is unclear whether cable infrastructure contributed to those decreases. Another investigative tool would be to look for possible harmful impacts of increased connectivity, such as cyber harms. For now, Australian cable projects continue to roll out across the Pacific.

We recommend that DFAT's Cable Connectivity and Resilience Centre should lead a significant step-up in Australia's engagement with European partners to exchange views on challenges and identify potential areas of policy cooperation.

8.5 Engagement with Pacific partners

For around a decade, the Australian Government has been actively working with partners in the Pacific to enhance cable resilience. While this assistance is being given in the context of geopolitical competition, Australia has had to work to tailor its assistance to the development needs of local partners.

Australia's engagement spans direct cable financing through the AIFFP, technical and policy support through DFAT's Cable Connectivity and Resilience Centre, and close coordination with key donor partners including the US, Japan, and New Zealand. This engagement reflects a broader recognition that Pacific cable resilience is inseparable from Australia's own strategic interests in the region, given the shared maritime domain and the risk that disruption to a neighbour's

connectivity can have flow-on effects for regional stability and Australia's own diplomatic and security relationships.

8.6 Engagement with Indian Ocean partners

While much of Australia's focus in international engagement on cables in recent years has been on building resilience in the Pacific, it faces similar vulnerabilities in the Indian Ocean. Indeed, Australia's westward cable connections, most of which currently run through Singapore and the Indonesia archipelago, are more vulnerable and have less redundancy compared with Australia's cable connections across the Pacific. As with the Pacific, the Indian Ocean is dominated by developing countries and numerous small island states with constrained resources. Many countries rely on only a small number of connections, including Chinese-built cables, that may create significant vulnerabilities. For example, Bangladesh, a country of some 180 million people, relies on just two or three submarine cables for a significant proportion of its international data needs.[116] It is in Australia's interests to work with Indian Ocean countries, using its experience in the Pacific, to help enhance regional resilience.

As the largest country in the region, India is likely to be an important partner for Australia in building Indian Ocean cable resilience. A first step would involve establishing formal mechanisms for consultation, monitoring, and information sharing between the countries. This should include building a shared language to identify and respond to attacks and practising responses. Second, the two can work with the cables industry to enhance maintenance arrangements. This could require contributing to the costs of repair vessels and depots to prioritise the repair of certain cables in a national emergency. Third, governments can work with the private sector to build a direct cable link between the two countries to mitigate vulnerabilities arising from reliance on the Singapore/Malacca route for communications. Last, and not least, the two countries should work with other Indian Ocean partners to create shared perspectives of threats, build redundancy, and encourage the use of trusted networks wherever possible.

8.7 Engagement with partners in Southeast Asia

Australia should work with partners to enhance the resilience of cable networks in Southeast Asia. In 2024, ASEAN established an ASEAN Working Group on Submarine Cables with the aim of strengthening the resilience, security, and repair efficiency of critical submarine telecommunications infrastructure in Southeast Asia.[117] It operates under the ASEAN Digital Ministers' Meeting framework and is chaired by Singapore's Infocomm Media Development Authority.

As the leading submarine cables hub in the region, Singapore is likely to be a key Southeast Asian partner for Australia on cable protection. As part of the Australia-Singapore Digital Economy Agreement, the two countries have already agreed to keep any permit application processes for submarine cables reasonable, transparent, and as swift as possible, and to only charge reasonable fees. Additionally, each side can use any supplier they select, avoiding any protectionist practices. Furthermore, both also commit to reducing the risk of damage to the other party's cables, with room to choose how they do it. There is considerable scope for Australia to work with ASEAN and individual partners in Southeast Asia, including through joint exercises to improve monitoring and response as well as support for streamlining regulatory processes.

Australia cannot protect its submarine cable network alone. The transnational nature of cables – crossing multiple jurisdictions and spanning vast distances – means that effective protection requires sustained engagement with industry, regional partners, and close allies. The partnerships and frameworks discussed in this section, from the Quad and AUKUS to European engagement and Pacific connectivity initiatives, we believe provide the building blocks for a coordinated regional approach. Translating these into effective operational cooperation, shared surveillance capabilities, and coordinated incident response should be a central element of an Australian national submarine cable strategy.

Towards a national submarine cable strategy

Australia lacks a comprehensive national strategy with a roadmap for pursuing opportunities and building resilience in its national submarine cable system. The purpose of this section is to consider why the Australian Government should adopt a national submarine cables strategy as part of a broader emphasis on building "whole-of-nation" resilience. It includes the following subsections:

9.1 Why does Australia need a national submarine cable strategy?

9.2 What have other countries done in this area?

9.3 Key issues to be addressed in an Australian national strategy

9.1 Why does Australia need a national submarine cable strategy?

Australia's current approach to its submarine cables network is disjointed and ad hoc. For example:

- there is no clear national statement of risks in relation to Australia's cable network, or the potential economic opportunities for Australia of enhancing the network
- there are few formal mechanisms for a joined-up approach to policy formulation among relevant government agencies
- there are no formal mechanisms for liaison between government and cable operators
- there are significant gaps in maritime law enforcement powers in respect of cables
- regulatory powers over private operators may not be adequate to mitigate threats
- there is no clear and agreed allocation of roles and responsibilities among government agencies, including which agencies should take a leading role in relation to certain issues
- there is no clear and agreed allocation of responsibilities for threat detection and response as between private operators and government agencies
- there are no formal mechanisms for a coordinated operational response at a national level, meaning that responses may default to local law enforcement even in cases of state-based threats
- there is no commitment to allocate resources to meet agency responsibilities, including in monitoring and response.

There is much to be done.

While the principal focus of *Connected & protected* is on security threats to submarine cables, it should be noted that frequently the same policy settings that enhance security, including permitting, expanded protection zones, clear agency responsibilities, and a welcoming regulatory environment, are also the settings that attract investment. Getting this right is therefore both a security imperative and an economic opportunity. Indeed, there is growing international recognition of the value of national-level strategies for cables. In February 2026, the International Telecommunication Union's International Advisory Body on Submarine Cable Resilience, on which Australia is represented through DFAT's Cable Connectivity and Resilience Centre, adopted recommendations encouraging governments to develop national-level strategies informed by data on submarine cable faults, risks and vulnerabilities.

A national submarine cable strategy aimed at building resilience would also be consistent with the Australian Government's increased emphasis on taking a 'whole-of-nation' approach towards building national resilience towards a range of potential threats.

9.2 What have other countries done in this area?

In recent years, several of Australia's international partners have adopted strategies to further submarine cable security, some more

comprehensive than others. Australia can learn much from the approaches taken in both Europe and the US.

France

France is leading much of the thinking on cables as part of seabed warfare. In 2022, the French Ministry of Armed Forces released a national *Seabed Warfare Strategy* that focuses on securing, monitoring, and controlling undersea infrastructure to ensure digital sovereignty, national security, and economic interests.[118] The strategy involves protecting critical data cables from sabotage, enhancing seabed surveillance down to 6,000 meters, and fostering domestic industrial capabilities through state-controlled companies such as ASN. The strategy is not limited to areas within French jurisdiction and encompasses areas that lie beyond national jurisdiction as long as they are of operational and national interest. The strategy is coordinated through the General Secretariat for Defence and National Security, which is an interministerial body under the prime minister.

The strategy specifies that the "seabed is not a compartment or a field in its own right" but is, nonetheless, a "new area of conflict". The key end-objectives of the strategy have been outlined as:

- guarantee freedom of action for France's armed forces in the air-maritime environment
- contribute to the protection of France's underwater installations (including submarine communication cables)
- guarantee French interests in the exploration and exploitation of mineral and energy resources, in particular in areas under national jurisdiction
- while being capable of posing a credible threat to the interests or forces of a potential enemy tempted to attack the interests of France or its strategic partners.[119]

European Union

Following the French lead, the EU adopted an *Action Plan on Cable Security* in 2025.[120] Pursuant to the plan, a Cable Security Toolbox was adopted in 2026 that provides a 'toolbox' of mitigating measures to identified threats, vulnerabilities, and dependencies, proposes a list of new strategic cable projects with public funding, and proposals for maintenance and repair arrangements.[121]

United Kingdom

In December 2025, the UK Government announced that it had set up a new cross-government body to coordinate policy on subsea cables in response to a report by the Joint Committee on the National Security Strategy.[122] The committee had recommended the government "provide a joined-up subsea cables function" to bring together different government departments and agencies responsible for operations, security, policy, resilience, and contingency planning.[123] The UK Government has agreed with these key recommendations.

United States

The US does not have a single comprehensive cable strategy, but is pursuing several initiatives to enhance its own cable security as well as an international 'Trusted Network' strategy.

The US Federal Communications Commission has adopted several new regulations that give the US Government much greater control over cables landing in the country. This includes a 'presumption of denial' for the licensing of new US-connected cables involving entities controlled by foreign adversaries (including equipment suppliers). An interagency Committee for the Assessment of Foreign Participation (known as 'Team Telecom') under the control of the National Security Division of the Department of Justice was established to advise on licensing applications. In some cases, operators must enter into a Network Security Agreement that may include obligations to locate a primary or secondary NOC in the US, which would potentially give the US Government greater access to the systems.

The US Government has also focussed on sovereign repair capabilities. In 2019, it established a program to build a Cable Security Fleet of US-flagged cable-laying and repair ships (although this program was defunded in 2024 and its future is uncertain). Congress is currently considering a law to enhance the US Government's powers over submarine cables.

Since 2021, the US Department of State, through its CABLES Program, has pursued the 'Trusted Network' strategy to reduce China's role (and enhance the role of US companies) in cable networks in the Indo-Pacific and elsewhere.[124] The CABLES Program now forms part of the State Department's 2024 *International Cyberspace & Digital Policy Strategy,* which is a comprehensive policy of exercising US influence across the entire digital ecosystem, including hardware, software, protocols, technical standards, providers, operators, users, and supply chains spanning telecommunication networks and undersea cables. A key line of effort in the 2024 strategy is enhancing the security and resilience of undersea cables.

According to the strategy: "Choices made about which vendors to rely on for undersea cable infrastructure, maintenance, and repair operations can either drive development and innovation or lead to new forms of dependency and insecurity. As a result, the Department of State, in coordination with other agencies, will prioritize enhancing the security and resilience of undersea cables … The US Government will continue to support US and other trusted suppliers in the installation, operation, maintenance, and repair of secure infrastructure". [125]

Pursuant to this strategy, over the last several years, the US Government has used multiple levers to ensure that investments in new cables involve trusted networks and suppliers. This includes using US diplomatic influence to lobby investors; 'capacity building' programs for national telecommunications companies to encourage the use of US equipment suppliers over Chinese suppliers (e.g. SEA-ME-WE 6);[126] and direct funding of cable projects using non-Chinese suppliers (such as US grants to help fund the East Micronesia Cable to be built by a Japanese firm). Perhaps the most effective lever is (informal) pressure on US-based technology companies not to use 'untrusted' networks anywhere in the world for their data transmission needs, which in many cases would threaten the economic viability of a cable project.

9.3 Key issues to be addressed in an Australian national strategy

The following builds on and extends the priority recommendations set out in the Executive Summary, detailing the fuller architecture of an Australian national strategy. We recommend that consideration should be given to a national strategy that addresses the following issues.

1. Submarine cable investment policy

Include policies to actively promote Australia as an Indo-Pacific preferred cable hub, recognising that attracting new cable investment directly enhances digital resilience. Key levers would include streamlined permitting, expanded CPZs, and clear regulatory settings. The security agenda and the economic opportunity agenda are, in this respect, the same agenda.

2. Identify security threats and mitigation strategies

Identify potential threats and vulnerabilities to Australia's cables network, major risk scenarios, and potential mitigation strategies (potentially using the EU's 'toolbox' approach).

3. Allocation of responsibilities among relevant Australian agencies

The strategy should clearly allocate responsibilities for the security of Australia's cables network among relevant federal and state agencies, including the designation of civil and military agencies in leading and supporting roles in respect of specified threats.

4. Interagency policy and operational coordination mechanism

The strategy should establish a high-level interagency coordination committee among relevant agencies to coordinate policy and operational responses. The committee would be chaired by MBC and be required to report regularly to the Secretaries Committee on National Security on threat developments and network security.

5. Government-private operator coordination mechanism

The strategy should establish an advisory board including Australian cable network operators and other industry stakeholders that would support the interagency committee as well as informing relevant line agencies.

6. Resourcing of responsible agencies

Adequate resourcing includes commitments for human resources and capabilities for relevant agencies, particularly MBC and the ADF, to fulfil designated responsibilities, including in monitoring, detection, and response.

7. Update legal regime

A commitment to undertake a public review of Australia's legal regime for the protection of submarine cables, among other things, to:

- ensure that regulators have adequate legal authority to require private operators to take action to mitigate threats, including in the design and routing of cables
- give the Australian Government greater access or control over cable systems in the event of a contingency
- ensure that law enforcement agencies have the maximum possible powers necessary to act against any person who seeks to disrupt submarine cables, whether inside or outside areas of direct legal jurisdiction.

8. Enhancing physical cable protection and promoting monitoring and surveillance capabilities

Set out approaches for the deployment of physical cable protection measures, as well as enhancing monitoring and surveillance of the network, including the use of integrated cable monitoring systems. The strategy should also address the integration of ADF capabilities into cable protection, including seabed surveillance and maritime domain awareness, ASW, counter-UUV, clearance diving and mine countermeasures, ensuring these capabilities keep pace with the modern threat environment and that clear doctrine exists for deployment in cable protection scenarios.

9. Enhancing cable redundancy and geographic and ownership diversity

One of the most effective ways of mitigating the risk of intentional disruption to Australia's network is to ensure redundancy and geographic diversity of routes and landing points. The strategy should also explicitly address diversity in cable ownership and operation. Cables operated by wholly Australian-owned companies carry a different risk profile from those operated by foreign consortia or hyperscalers, as the former are more directly subject to Australian legal obligations and government direction and may be more reliably available to support national priorities in a crisis. The strategy should consider how to encourage and sustain a viable cohort of Australian-owned operators as a resilience asset in its own right.

10. Ensuring timely access to cable repair capabilities

The cable industry's cable maintenance agreements do not include commercial structures that prioritise the order of repairs in the event of a significant single event that causes disruption to multiple cables. The strategy should set out a preferred approach for ensuring timely access to cable repair capabilities (including expertise, equipment, and spares) in cases of national emergency. This may include a mix of sovereign capabilities and stockpiles and arrangements for priority access to private capabilities.

11. Ensuring access to satellite connectivity

Ensure that there is adequate access to satellite communications connectivity as a partial back-up in case of widespread disruption to Australia's cable network. This would require accountability for funding and clear understandings on traffic prioritisation.

12. Mitigating cyber risks

Cyber-attack may be one of the greatest threats faced by Australia's cables network, including attacks on network management systems, cable landing stations, wet infrastructure, and cable maintenance vessels. Key actions/issues that could be addressed in a national strategy include the following.

- Designating ASD as the lead technical authority for the cyber security of submarine cable systems, providing threat intelligence, advice and incident response support directly to cable operators.
- Requiring, through the *Security of Critical Infrastructure Act* framework administered by the Department of Home Affairs, that all new submarine cable systems landing in Australia are built secure-by-design, closing the current gap in the SOCI regime.
- Mandating, under the same framework, cyber security exercises and vulnerability assessments for cable systems designated as Systems of National Significance.
- Developing guidance for cable operators on securing remote network management systems, including access controls, vendor management, and software update protocols.
- Promoting the adoption of post-quantum cryptography for data in transit across submarine cable systems, in anticipation of future quantum computing threats.

13. Regional and international engagement strategies

Set out a regional engagement strategy with partners in Southeast Asia and the Pacific and Indian oceans with the aim of promoting mutual capabilities and resilience with regional partners. The strategy should also set out a broader international engagement strategy for Australia to work together with key regional partners in capability building and coordinated incident response. Vital to such engagement would be continued funding for DFAT's Cable Connectivity and Resilience Centre and the AIFFP, which underpins Australia's regional engagement and supports strategic submarine cable projects for neighbours respectively.

14. Connecting Antarctica

Include a commitment by the Australian Government to work towards developing cable connectivity with Australia's research stations in Antarctica and Macquarie Island.

15. Related seabed infrastructure

Address the protection of related seabed infrastructure, including power cables, pipelines, and other critical seabed assets. As Australia's offshore energy sector expands and new categories of seabed infrastructure are deployed, including offshore wind farms, the threat environment and response capabilities relevant to submarine cables will increasingly apply to this broader infrastructure picture.

16. Deterrence doctrine

Indicate Australia's approach to deterring potential adversaries from disrupting Australia's submarine cable network. Effective deterrence requires demonstrated detection and attribution capability, clear response thresholds, and a willingness to impose costs on those who attack Australian infrastructure. Given the attribution challenges posed by hybrid tactics, Australia's deterrence posture should be developed and exercised in close coordination with allies.

References

1. Richard Marles, "Address to the 2026 Shangri-La Dialogue: Plenary Session Three," speech, Department of Defence, Singapore, May 30, 2026, https://www.minister.defence.gov.au/speeches/2026-05-30/address-2026-shangri-la-dialogue-plenary-session-three
2. Department of Industry, Science, Energy and Resources, *Australia's digital trust report* (Canberra, 2020), https://www.austcyber.com/resource/digitaltrustreport2020
3. Andrew Colley, "SUBCO reveals first Australia–US direct undersea cable to go live late 2028," *ITnews*, January 20, 2026, https://www.itnews.com.au/news/subco-reveals-first-australia-us-direct-undersea-cable-to-go-live-late-2028-623041
4. "Antarctic SMART Cable," *Submarine Cable Networks*, https://www.submarinenetworks.com/en/systems/antarctic/antarctic-smart
5. Joint Parliamentary Committee on the National Capital and External Territories, *Inquiry into the Availability and Access to Enabling Communications Infrastructure in Australia's External Territories: Terms of Reference*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/National_Capital_and_External_Territories/ETCommsInfra/Terms_of_Reference
6. Australian Antarctic Division, *Submission to the inquiry into the availability and access to enabling communications infrastructure in Australia's external territories*, Submission 31 (2021)
7. Bureau of Meteorology, *Submission to Inquiry on the Availability and Access to Enabling Communications Infrastructure in Australia's External Territories*, Submission 30 (2021)
8. In March 2026, Salience Consulting DMCC & Pioneer Consulting Holdings LLC completed a significant report for Chilean Subsecretariat of Telecommunications (SUBTEL) on the proposed Chilean Antarctic cable (see https://www.submarinenetworks.com/en/systems/antarctic/chile-antarctic-cable/first-definitions-on-the-antarctic-cable). The project is still in the feasibility stage.
9. National Science *Foundation, Exploring the Feasibility of a Science Monitoring and Reliable Telecommunications (SMART) Fiber Optic Cable System Connecting Antarctica, Australia and New Zealand* (2023), https://nsf-gov-resources.nsf.gov/files/NSF-Public-Release-DTS-Final.pdf; National Science Foundation, *Request for Information (RFI) on Science Research Goals/Objectives Affecting Proposed U.S. Antarctic Science Monitoring and Reliable Telecommunications (SMART) Cable and Route Design* (2024), https://www.federalregister.gov/documents/2024/11/21/2024-27292/request-for-information-rfi-on-science-research-goalsobjectives-affecting-proposed-us-antarctic
10. National Science Foundation, *Request for Information (RFI): Development of an Antarctic Subsea Telecommunications Cable for Science* (2024), https://www.submarinenetworks.com/en/systems/antarctic/antarctic-smart/us-nsf-requests-for-information-on-antarctic-smart-cable
11. Jocelinn Kang and Jessie Jacob, *Connecting the Indo-Pacific: The Future of Subsea Cables and Opportunities for Australia*, Australian Strategic Policy Institute, September 2024, https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/
12. US companies typically design components and outsource manufacture.
13. Melissa Mahe, "Subsea Cables and US National Security," *Steptoe Risk Outlook,* August 8, 2025
14. Office of Public Affairs, "Team Telecom recommends FCC grant Google and Meta licenses for undersea cable," media release, Department of Justice, US Government, December 17, 2021, https://www.justice.gov/archives/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable
15. Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, Center for Strategic and International Studies, February 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition
16. Joe Brock, "U.S. and China wage war beneath the waves – over internet cables," *Reuters,* March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/
17. Elina Noor, "Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed", *Carnegie Endowment,* December 18, 2024, https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables
18. Elina Noor, "Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed", *Carnegie Endowment,* December 18, 2024. https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables

19. Australian Infrastructure Financing Facility for the Pacific, "Investments," https://www.aiffp.gov.au/investments

20. "Google to build undersea cables in Papua New Guinea under Australia defence treaty," *ABC News,* December 13, 2025, https://www.abc.net.au/news/2025-12-13/google-building-undersea-cables-in-png/106139500

21. "Congress presses Google, Meta, Microsoft, Amazon over Chinese tech in US bound subsea cables." *Industrial Cyber,* July 22, 2025, https://industrialcyber.co/critical-infrastructure/congress-presses-google-meta-microsoft-amazon-over-chinese-tech-in-us-bound-subsea-cables/

22. Kang and Jacob, *Connecting the Indo-Pacific*

23. Dan Swinhoe, "Submarine cables find new impetus under hyperscalers," *Data Center Dynamics*, November 23, 2021, https://www.datacenterdynamics.com/en/analysis/submarine-cables-find-new-impetus-under-hyperscalers/

24. Manish Singh, "Facebook, telcos to build huge subsea cable for Africa and Middle East," *TechCrunch,* May 14, 2020, https://techcrunch.com/2020/05/14/2africa-africa-middle-east-facebook-subsea-cable/

25. In comparison, the newly installed MAREA trans-Atlantic cable is capable of carrying 224 Tbps (or 224,000 Gbps)

26. Debra Werner, "University of Western Australia unveils optical ground network," *Space News*, October 2, 2025, https://spacenews.com/university-of-western-australia-unveils-optical-ground-network/

27. "Submarine Cables – International Framework," National Oceanic and Atmospheric Administration, https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-international-framework

28. *Union Steamship Co of Australia Pty Ltd v King* (1988) 166 CLR 1

29. Bikash Koley, "Introducing the TalayLink subsea cable and new connectivity hubs," *Google Cloud Blog*, November 24, 2025, https://cloud.google.com/blog/products/infrastructure/talaylink-subsea-cable-to-connect-australia-and-thailand

30. Rocco Cartusciello, "YL Blog #120 – Underwater Frontlines: China's Cable-Cutting Threat in the South China Sea," *Pacific Forum*, May 30, 2025, https://pacforum.org/publications/yl-blog-120-underwater-frontlines-chinas-cable-cutting-threat-in-the-south-china-sea/

31. Alistair Bates and Mietta Adams, "Google's global data hub plan for Christmas Island gets mixed reviews from locals," *ABC News*, November 29, 2025, https://www.abc.net.au/news/2025-11-29/google-data-centre-stokes-uncertainty-on-christmas-island/105984092

32. Australian Government Department of Defence, *2026 National Defence Strategy and 2024 Integrated Investment Program*, https://www.defence.gov.au/about/strategic-planning/2026-national-defence-strategy-2026-integrated-investment-program

33. Australian Government, *Civil Maritime Security Strategy* (2021), https://www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf

34. Australian Government, *2023–2030 Australian Cyber Security Strategy* (2023), https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

35. Australian Border Force, "Counter 8 civil maritime security threats," *Maritime Border Command*, https://www.abf.gov.au/about-us/what-we-do/border-protection/maritime/civil-maritime-security-threats

36. Section 474.6 of the *Criminal Code Act 1995* makes it a Commonwealth offence to tamper with, interfere with, or hinder the operation of equipment or facilities owned by a carrier or carriage service provider.

37. Section 5 of the *Coastal Waters (State Powers) Act 1980*.

38. Winston Qiu, "Submarine Cables Cut after Magnitude - 9.0 Earthquake and Tsunami in Japan," *Submarine Cable Networks*, March 12, 2011

39. C. Sinadinovski, T. Jones, D. Stewart, and N. Corby, "Earthquake history, regional seismicity and the 1989 Newcastle earthquake," in *Earthquake Risk in Newcastle and Lake Macquarie*, Geoscience Australia, 2002, https://pid.geoscience.gov.au/dataset/ga/40255

40. Alan Mauldin, "Cable Breakage: When and how cables go down," *TeleGeography,* May 3, 2017, https://blog.telegeography.com/what-happens-when-submarine-cables-break

41. "From Australia to Zimmermann: A Brief History of Cable Telegraphy during World War One," *Innovating in Combat*, https://blogs.mhs.ox.ac.uk/innovatingincombat/files/2013/03/Innovating-in-Combat-educational-resources-telegraph-cable-draft_FIN.pdf

42. Robert Onfray, "The Cable Cutters," August 11, 2023, https://www.robertonfray.com/2023/08/11/the-cable-cutters/

43. In February 2024, three cables were cut off Djibouti. While Houthi rebels were initially blamed for the incident, according to later reports the damage was caused by a British cargo vessel *Rubymar*, which was abandoned by its crew after a Houthi attack and left to drift while dragging its anchor before it sank. The Houthis officially denied allegations that they had intentionally cut the cables. In September 2025, four cables in the Red Sea were cut, probably by a ship dragging its anchor.

44. Jordan Robertson and Drake Bennett, “A Subsea Cable Went Missing: Was Russia to Blame?”, *Businessweek,* July 11, 2024

45. Niels Nagelhus Schia, Lars Gjesvik, and Ida Rødningen, “The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?,” *Norwegian Institute of International Affairs, Policy Brief*, 1/2023, https://www.nupi.no/content/pdf_preview/26372/file/NUPI_Policy_Brief_1_23_Schia_Gjesvik_R%C3%B8dningen-FERDIG.pdf

46. Olivia Ireland, Thomas Copeland, and Frank Gardner, “UK says Russia ran submarine operation over cables and pipelines” *BBC,* April 10, 2026. https://www.bbc.com/news/articles/cre13qn9z7do

47. Roderich Kiesewetter, “Deutschland verweilt im Dornröschenschlaf,” *Common Ground of Europe*, December 14, 2023, http://commongroundeurope.eu/blog/roderich-kiesewetter-deutschland-verweilt-im-dornroeschenschlaf/

48. Meaghan Tobin and Vic Chiang, “Internet outage has Taiwan worried about threat from Chinese sabotage,” *The Washington Post*, March 9, 2023, https://www.washingtonpost.com/world/2023/03/09/taiwan-matsu-internet-access-china-fishing

49. Ray Powell (@GordianKnotRay), “IT’S LEAVING! ...,” X post, January 14, 2025, https://x.com/GordianKnotRay/status/1878953699617468488

50. Aurelia Insisa, *What Lies Beneath: Hybrid Threats to Taiwan’s Submarine Cables and the Contest in the Information Domain*, Istituto Affari Internazionali, January 2026, https://www.iai.it/sites/default/files/iaip2601.pdf

51. “Chinese captain convicted of damaging undersea cable deported,” *Taipei Times,* January 9, 2026, https://www.taipeitimes.com/News/taiwan/archives/2026/01/09/2003850330

52. Insisa, *What Lies Beneath*

53. Winston Qiu, “Taiwan Amends Seven Submarine Cable Laws, up to 7 Years in Prison for Intentional Damage,” *Submarine Cable Networks,* October 31, 2025

54. Taiwan Ministry of Foreign Affairs, *Risk Management Initiative on International Undersea Cables*, October 28, 2025, https://ws.mofa.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNDAyL3JlbGZpbGUvNzQvMTIwOTcwLzkyNjk5NmU2LTE5NWMtNGEyNy1hY2YxLTg4Y2I5NTUxNDhkNC5wZGY%3D&n=5rW357qc5YCh6K2w5Y6f5paHLnBkZg%3D%3D

55. “Taiwan’s submarine cable network strategic value and outlook,” *Taiwan News,* February 28, 2025, https://www.taiwannews.com.tw/news/6048410; “Taiwan to Build Five New Undersea Cables to Bolster Network Resilience,” *Subsea Cables*, December 26, 2025, https://www.subseacables.net/industry-news/taiwan-to-build-five-new-undersea-cables-to-bolster-network-resilience/

56. Matt Burgess, “The Unsolved Mystery Attack on Internet Cables in Paris,” *Wired*, July 22, 2022, https://www.wired.com/story/france-paris-internet-cable-cuts-attack/

57. Kushal Deb, “Hormuz is a digital chokepoint: How can the US-Iran war threaten internet connectivity?” *WION,* April 28, 2026, https://www.wionews.com/photos/irgc-subsea-cables-strait-of-hormuz-digital-chokepoint-1777373875901#goog_rewarded

58. Zelie Petit, “Beneath NATO’s Radars: Unaddressed Threats to Subsea Cables,” Center for Strategic and International Studies, December 2, 2024, https://www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables

59. Justin Sherman, *Cyber Defense Across The Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council, September 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

60. “Cyberattack against Hawaii undersea internet cable averted,” *SC Media*, April 14, 2022, https://www.scworld.com/brief/cyberattack-against-hawaii-undersea-internet-cable-averted; AJ Vicens, “DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii” *CyberScoop,* April 13, 2022, https://cyberscoop.com/undersea-cable-operator-hacked-hawaii/

61. Juha Saarinen, “Southern Cross cable hit by fault”, *ITnews,* November 9, 2012, https://www.itnews.com.au/news/southern-cross-cable-hit-by-fault-322426

62. Paul Godfrey, Simon Druker, and Ehren Wynder, “911 call centers back online after IT outage causes global chaos,” *United Press International*, July 19, 2024, https://www.upi.com/Top_News/World-News/2024/07/19/IT-failure-hits-causes-chaos-around-world/2531721376791#google_vignette

63. “Global IT outage: Computer havoc caused by CrowdStrike outage could take days to fix — as it happened,” *ABC News*, July 19, 2024, https://www.abc.net.au/news/2024-07-19/global-it-outage-crowdstrike-microsoft-banks-airlines-australia/104119960

64. International Maritime Organization, Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems

65. Henry M. Jackson School of International Studies, *Hidden Highways of the Internet: Global Subsea Cable Security*, 2025, https://jsis.washington.edu/nie/wp-content/uploads/2025/03/Task-Force-B-Final-Report.pdf

66. Associated Press, "New Nuclear Sub Is Said to Have Special Eavesdropping Ability," *The New York Times,* February 20, 2005, https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html

67. US Office of the Director of National Intelligence, *Threats to Undersea Cable Communications*, September 7, 2017, https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf

68. "Googleマップにもくっきり、中国製盗聴装置に狙われる沖縄海底ケーブルは「丸裸同然」," *JB Press*, July 21, 2024, https://jbpress.ismedia.jp/articles/-/82146?page=3

69. Yuka Koshino, *The Changing Submarine Cables Landscape: Expanding the EU's Role in the Indo-Pacific*, European Union Institute for Security Studies Brief, no. 19, October 2024, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2024-19_Submarine%20cables.pdf

70. JSIS, *Hidden Highways of the Internet*

71. Dustin Volz, Drew FitzGerald, Peter Champelli, and Emma Brown, "U.S. fears undersea cables are vulnerable to espionage from Chinese repair ships," *The Wall Street Journal*, May 19, 2024, https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320

72. Alexander Botting, Alexis Steffaro, and Luke O'Grady, *Shoring Up Subsea Security: A Comprehensive Action Plan to Promote Submarine Cable Resiliency, Security and Governance*, Center for Cybersecurity Policy and Law, September 2025, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68d4590cefdd47a519523ace_CCPL_SubseaWhitepaper_2025.09.pdf

73. Divij Bhaw, *Harvest Now, Decrypt Later: Securing Sea Lines of Communication in the Era of Quantum-Enabled Espionage,* UWA Defence and Security Policy Brief, February 11, 2026, https://defenceuwa.com.au/publications/policy-briefs/harvest-now-decrypt-later-securing-sea-lines-of-communication-in-the-era-of-quantum-enabled-espionage-2/

74. ODNI, *Threats to Undersea Cable Communications*

75. Submarine Cable Networks, "Stations," accessed December 5, 2025, https://www.submarinenetworks.com/en/stations

76. Sherman, *Cyber Defense Across the Ocean Floor*

77. Australian Cyber Security Centre, "Countering Chinese State-Sponsored Actors," August 28, 2025, https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system

78. David Swan, "Salt Typhoon hackers 'almost certainly' in Australia's critical infrastructure," *The Sydney Morning Herald*, January 2, 2026, https://www.smh.com.au/technology/salt-typhoon-hackers-almost-certainly-in-australias-critical-infrastructure-20251231-p5nqwn.html

79. Cybersecurity and Infrastructure Security Agency et al., "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-us-critical-infrastructure

80. Palo Alto Networks, "Harvest Now, Decrypt Later (HNDL): The Quantum-Era Threat," accessed December 11, 2025, https://www.paloaltonetworks.com.au/cyberpedia/harvest-now-decrypt-later-hndl

81. Chris C. Demchak and Yuval Shavitt, "China's maxim—leave no access point unexploited," *Military Cyber Affairs* 3, no. 1 (2018): 7

82. Demchak and Shavitt, "China's maxim."

83. Henry Birge-Lee, Maria Apostolaki, and Jennifer Rexford, "Global BGP Attacks that Evade Route Monitoring," arXiv, August 19, 2024, https://arxiv.org/abs/2408.09622

84. Australian Federal Police, "Ship captain charged over underwater cable damage off Perth," media release, August 21, 2021, https://www.afp.gov.au/news-centre/media-release/ship-captain-charged-over-underwater-cable-damage-perth

85. Lydia Hales, "Tasmania's internet outage caused by damaged Telstra cables demonstrates the state's vulnerability," *ABC News,* March 2, 2022, https://www.abc.net.au/news/2022-03-02/tasmania-reliance-on-undersea-cables-fails-again/100873280

86. Jonathan Gleeson, "Ship happens – repairing Australia's submarine internet lifelines," *Vocus*, March 2, 2025, https://www.vocus.com.au/vocus-blog/ship-happens-repairing-australias-submarine-internet-lifelines

87. Samantha Dick and Stephen Dziedzic, "Dutton says Chinese research ship is collecting intelligence, mapping undersea cables," *ABC News*, March 31, 2025, https://www.abc.net.au/news/2025-04-01/dutton-says-chinese-research-ship-mapping-undersea-cables/105122068

88. International Cable Protection Committee, *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, version 1.2, November 25, 2025, https://www.iscpc.org/documents/?id=3733

89. Alexander Botting, Alexis Steffaro, and Luke O'Grady, *Shoring Up Subsea Security: A Comprehensive Action Plan to Promote Submarine Cable Resiliency, Security and Governance*, Center for Cybersecurity Policy and Law, September 2025, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68d4590cefdd47a519523ace_CCPL_SubseaWhitepaper_2025.09.pdf

90. Ravi Nayyar, "Meta's Waterworth cable project is about geopolitics and geoeconomics," *The Strategist,* February 28, 2025, https://www.aspistrategist.org.au/metas-waterworth-cable-project-is-about-geopolitics-and-geoeconomics/

91. Bikash Koley, "Introducing Dhivaru and two new connectivity hubs," *Google Cloud Blog*, November 18, 2025, https://cloud.google.com/blog/products/networking/introducing-dhivaru-new-subsea-cable

92. Bikash Koley, "Introducing the TalayLink subsea cable and new connectivity hubs," Google Cloud Blog, November 24, 2025, https://cloud.google.com/blog/products/infrastructure/talaylink-subsea-cable-to-connect-australia-and-thailand

93. Giulia Bernacchi, "Australia Establishes Navy Unit for Maritime Autonomous Systems," *The Defense Post,* April 15, 2026. https://thedefensepost.com/2026/04/15/australia-unit-maritime-autonomous-systems/

94. Richard Marles, "Address to the 2026 Shangri-La Dialogue: Plenary Session Three," speech, Department of Defence, Singapore, May 30, 2026, https://www.minister.defence.gov.au/speeches/2026-05-30/address-2026-shangri-la-dialogue-plenary-session-three

95. Australian Government Department of Defence, "Undersea support vessel to deliver enhanced capability," media release, April 8, 2023, https://www.defence.gov.au/news-events/releases/2023-04-08/undersea-support-vessel-deliver-enhanced-capability

96. Samuel Bashfield, "Cable ties: Defending seabed lines of communication," *The Interpreter,* July 10, 2024, https://www.lowyinstitute.org/the-interpreter/cable-ties-defending-seabed-lines-communication

97. Mike Constable, Lane Burdette, and Alan Mauldin, "The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies," *TeleGeography*, June 2025, https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/The%20Future%20of%20Submarine%20Cable%20Maintenance_%20Trends%2C%20Challenges%2C%20and%20Strategies.pdf

98. International Cable Protection Committee, Presentation to the 2026 Plenary, January 2026.

99. ASEAN Cableship, "Cable Repair," https://www.aseancableship.com/news-achievements/cable-repair/

100. Global Marine, "Subsea cable maintenance," https://globalmarine.co.uk/services/subsea-cable-maintenance/

101. Olivier Pinaud, "Strategic submarine telecom cable manufacturer ASN nationalized by France," *Le Monde*, November 5, 2024, https://www.lemonde.fr/en/economy/article/2024/11/05/asn-strategic-manufacturer-of-submarine-telecom-cables-nationalized-by-france_6731573_19.html

102. Joint Committee on the National Security Strategy, *Subsea Telecommunications Cables: Resilience and Crisis Preparedness*, First Report of Session 2024–26, September 19, 2025, https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html

103. Robert Clark, "Japan, India govts ready to tip cash into cable ships – report", *Light Reading,* September 17, 2025, https://www.lightreading.com/cable-technology/japan-india-govts-ready-to-tip-cash-into-cable-ships-report

104. Australian Maritime Officers Union and Australian Institute of Marine and Power Engineers, *Building the Australian Strategic Fleet: Critical Next Steps to Bolstering Australia's Supply Chain Sovereignty,* July 2025, https://www.aimpe.asn.au/files/Australian_Shipping_Strategic_Fleet_Document_2025_V3.pdf

105. International Cable Protection Committee, *Government Best Practices*

106. International Advisory Body on Submarine Cable Resilience, *Working Group 3 Recommendations: Fostering Connectivity and Geographic Diversity*, https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2026/02/IAB-WG3-Recommendations.pdf

107. Julie Bishop, "Australia, US and Japan announce trilateral partnership for infrastructure investment in the Indo-Pacific," Export Finance Australia, https://www.exportfinance.gov.au/newsroom/australia-us-and-japan-announce-trilateral-partnership/

108. Samuel Bashfield and Rebecca Strating, "'Friendshoring' the seabed: Securing submarine cables through network centrality," *European Journal of International Security*, (2026), https://doi.org/10.1017/eis.2026.10042

109. "HEIST: A NATO SPS project," *NATO HEIST*, https://natoheist.org/Home.html

110. Amanda H.A. Watson, "Undersea cables: The official perspectives expressed in the Pacific region," *Marine Policy* 178 (August 2025): 106735, https://doi.org/10.1016/j.marpol.2025.106735

111. Kristi Govella, "Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience," *Marine Policy* 180 (October 2025): 106809, https://doi.org/10.1016/j.marpol.2025.106809

112. Watson, "Undersea cables," 106735

113. In the case of CS2, PNG's then-communications minister and Australia's then-prime minister forecast consumer price reductions for PNG and Solomon Islands respectively. "Cable to PNG and Solomons described as transformative," RNZ, April 19, 2018, https://www.rnz.co.nz/news/pacific/355485/cable-to-png-and-solomons-described-as-transformative

114. Amanda H.A. Watson, Picky Airi, and Moses Sakai, "No fall in mobile internet prices in PNG," *Devpolicy Blog*, April 19, 2022, https://devpolicy.org/no-fall-in-mobile-internet-prices-in-png-20220419/

115. Amanda H.A. Watson and Moses Sakai, "Mobile internet prices falling in Papua New Guinea," *Devpolicy Blog*, March 20, 2024, https://devpolicy.org/mobile-internet-prices-falling-in-papua-new-guinea-20240320/

116. David Brewster, Mike Constable, Syed Misbah Uddin Ahmad, Shahriar Khosnoor Prince, and Anthony Bergin, *Bangladesh's undersea critical infrastructure: an assessment of risks and vulnerabilities*, ANU National Security College, 2025

117. Association of Southeast Asian Nations, *ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables*, https://asean.org/wp-content/uploads/2012/05/ASEAN-Guidelines-for-Strengthening-Resilience-and-Repair-of-Submarine-Ca....pdf

118. French Ministry of Armed Forces, Seabed Warfare Strategy (2022), https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

119. Seabed Warfare Strategy, 27

120. European Commission, Joint Communication to the European Parliament and the Council, *EU Action Plan on Cable Security,* February 21, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009

121. European Commission, *Security and Resilience of EU Submarine Cable Infrastructures: Mapping, Risk Assessments, Stress Tests*, October 2025, https://ec.europa.eu/newsroom/dae/redirection/document/120904

122. Joint Committee on National Security Strategy, "Government strengthens undersea cables coordination following Committee report," December 18, 2025, https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/211009/government-strengthens-undersea-cables-coordination-following-committee-report/

123. Joint Committee on the National Security Strategy, *Subsea Telecommunications Cables: Resilience and Crisis Preparedness*, First Report of Session 2024–26, HC 723 / HL Paper 179, https://committees.parliament.uk/publications/49566/documents/264088/default/

124. US Department of State, *United States International Cyberspace and Digital Policy Strategy,* May 6, 2024, 27, https://2021-2025.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

125. *United States International Cyberspace and Digital Policy Strategy.*

126. Joe Brock, "U.S. and China wage war beneath the waves – over internet cables," *Reuters*, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/

Australian National University | NATIONAL SECURITY COLLEGE

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

@NSC_ANU

ANU National Security College

@anunationalsecuritycollege

@nscanu.bsky.social

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002

(Australian University)

Subscribe to our mailing list

Scan the QR code or visit **tinyurl.com/nsc-newsletters**

Subscribe to the National Security Podcast

Scan the QR code or visit **tinyurl.com/NatSecPod-NSC**